UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	No. 2:11-cr-00070-RAJ
	)	
	)	
vs.	)	Seattle, WA
	)	
ROMAN V. SELEZNEV,	)	
	)	Jury Trial, Day 2
Defendant.	)	August 16, 2016

VERBATIM REPORT OF PROCEEDINGS
BEFORE THE HONORABLE JUDGE RICHARD A. JONES
UNITED STATES DISTRICT COURT

APPEARANCES:

FOR THE PLAINTIFF:

NORMAN McINTOSH BARBOSA
U.S. Attorney's Office
700 Stewart Street, Suite 5220
Seattle, WA 98101-1271
norman.barbosa@usdoj.gov

C. SETH WILKINSON
U.S. Attorney's Office
700 Stewart Street, Suite 5220
Seattle, WA 98101-1271
seth.wilkinson@usdoj.gov

HAROLD W. CHUN
U.S. Department of Justice
1301 New York Avenue NW, Suite 600
Washington, DC 20005
harold.chun@usdoj.gov

FOR THE DEFENDANT: JOHN HENRY BROWNE
Law Office of John Henry Browne
108 South Washington Street, Suite 200
Seattle, WA 98104
johnhenry@jhblawyer.com

EMMA SCANLAN
Law Office of John Henry Browne
108 South Washington Street, Suite 200
Seattle, WA 98104
emma@jhblawyer.com

Andrea Ramirez, CRR, RPR
Official Court Reporter
United States District Court
Western District of Washington
700 Stewart Street, Suite 17205
Seattle, WA 98101
andrea_ramirez@wawd.uscourts.gov

Reported by stenotype, transcribed by computer

I N D E X

E X H I B I T S

THE CLERK: We are resuming our jury trial in the matter of the United States vs. Roman Seleznev, Cause Number CR11-70, assigned to this court.

THE COURT: Good morning, ladies and gentlemen of the jury.

As you recall, yesterday we closed the first day of trial with the government presenting their opening remarks. I now invite you to give your undivided attention to Mr. John Henry Browne, as he gives his opening remarks on behalf of Mr. Seleznev.

Counsel?

MR. BROWNE: Good morning, Your Honor. Good morning, everybody. Good morning.

Well, you're probably going to be happy to hear that I'm only going to probably talk to you about five or ten minutes.

As the judge explained to you, a couple times now, a defendant in a criminal case has no obligation to make an opening statement. You're going to hear me emphasize that word a few times, "statement," until the close of the government's case, or now. In fact, I was thinking about not doing it until later, but I decided to go ahead and make a few remarks this morning. I hope you don't think the time involved in these remarks has anything to do with the quality of these remarks.

So the first thing that's really important, first of all, it's really -- Judge Jones has not given you your notebooks.

And one of the reasons for that is because of the next thing I'm going to tell you is -- which is really important -- is what attorneys say or do is not evidence. What we say is not evidence. I don't think we can stress that more.

Yesterday, counsel for the government gave a presentation. And a couple of times during that presentation, the evidence will show that there were some errors, seemingly meaningless errors. But the evidence in this case is going to show you that, for instance -- I don't have the graphic in front of me, but you'll remember it. And believe me, by the time this is over, you're going to see it a lot, the graphic of the computers and the servers and all that. He said, pointing at the HopOne server, "And here's the 11-digit number." Well, I'm not the best at math, but I looked at it, and it's a 9-digit number. And that's what the evidence will show you.

And what you're going to learn in this trial and -- it's going to be a lot of technical testimony, lots. That's why if you do feel like taking notes, it's probably a good idea. But of course, as the judge said, that's up to you completely.

There's going to be a lot of technical evidence in this case. And a simple mistake like that, in a case when you're having supposed experts testifying about sophisticated computer tracking information, making a mistake as to whether a number is nine numbers or 11 numbers, the evidence will show you, is pretty huge. The evidence will show you that that is not 11.

It's nine. And there will be some other errors. That's why what we say is not evidence. What we say is based on what we think. You see all the books over there. You can see how much information there is in this case. Not to scare you, but there's a lot of information in this case.

Another example why what we say is not evidence is, yesterday there was some remark that there was an e-mail request to purchase an airplane ticket from Vladivostok to Bali. But when you see that evidence, you'll realize that's not true. It's an airline ticket that goes from Bali to Singapore. It's just the -- the detail in this case is going to be excruciating, but really important.

The other thing -- I'm almost done, actually -- I wanted to tell you is, when the judge asked the government to read off the witness list, there was a lot of names, as you recall, and then asked us, and Ms. Scanlan got up and mentioned the name of Eric Blank, who is -- may testify. Because as you've been told, the defense has no burden to put on a case whatsoever.

If we choose to, we may call Eric Blank. He's an expert, law enforcement background, recognized expert throughout the United States, if not the world. And he's an expert in computer specifics. The reason I mention that is because this case, more than many, is -- involves the cross examination of the government's witnesses.

What is the defense case? This is an opportunity, as the

judge says, to make remarks, not argument. And I don't intend to argue or point fingers or anything. The purpose of this is to make a statement. And the statement is, the defense case in this trial will be almost exclusively the cross examination of the government's witnesses and their testimony concerning very technical matters.

So the last thing, I'll just say it again -- and then I won't say it again -- evidence comes from the witness stand and anything that Judge Jones admits, the physical evidence. That's where evidence comes from, not from my mouth, not from counsel's mouth. And the fact that you don't have your notebooks is a really good example of that.

Then the last thing I want to tell you is, this is going to be not a really long trial, because all of us in here have been in a lot longer trials, but it's going to be a rather long trial, and it's going to be very, very technical in many ways.

So I just want to thank you for all of us, in advance. Because doing this is your civic duty, and a lot of people don't do that and get out of jury service any way they can. And we're very, very grateful that you've taken time out of your lives to do this very important matter, which is being watched closely by the whole world.

So I really thank you for your attention. That's really all I wanted to say. I wasn't going to say anything. I decided that I would. Thank you very much.

Thank you, Your Honor.

THE COURT: Thank you, Counsel.

Members of the jury, your notebooks and pens will be passed out at this time.

And just a word of caution, if at any point in time you run out of paper or need additional pens, you're not expected to wait until the break or recess. Just merely raise your hand, and we'll make that accommodation immediately.

One other thing I want to explain to you, you can see that you have monitors in front of you. During the course of the trial -- I'll wait until the notebooks are passed out.

Okay. Everyone has their government-issued pens and paper. Now you're ready to go.

I want to explain to you about how the monitors work. During the course of the trial, I fully expect that there's going to be quite a bit of evidence that's going to come through the government showing a document to a witness on an overhead. And then it's available for the witness to see, and I can see it, and the lawyers can see it, but you can't see it.

The way the process works is, a document is marked for identification, then it's shown to a witness. There may be some preliminary testimony about the document to establish the foundation for that document to be admitted. Once either side offers an exhibit then the Court has to make a firm ruling that says, "It's admitted." Once it's admitted, then the lawyers

will probably -- should be asking the Court for permission to publish to the jury. Once that permission is granted, only then do they display the document or exhibit before you.

So don't be troubled by the fact that a witness is being examined about a document that's not on your monitor. Until it's formally admitted, only then will you be allowed to see the exhibit at that point in time. Sometimes I'll see jurors looking or waving their hands saying, "We can't see it." There's a reason you can't see it. Once it's admitted, then you will be able to see it.

Counsel for the government, call your first witness.

MR. BARBOSA: Thank you, Your Honor.

The United States calls Deputy Assistant Director David Iacovetti.

THE COURT: Please step forward, sir.

DAVID IACOVETTI, having been duly sworn, was examined and testified as follows:

THE CLERK: Have a seat.

If you could please state your first and last names, and spell your last name for the record.

THE WITNESS: David Iacovetti. That's I-A-C-O-V-E-T-T-I.

THE COURT: You may inquire.

MR. BARBOSA: Thank you, Your Honor.

DIRECT EXAMINATION

BY MR. BARBOSA

Q Good morning, Mr. Iacovetti.

Could you tell the jurors where you work?

A Sure. Good morning. I work for the United States Secret Service, in Washington, D.C.

Q And where are you currently stationed?

A Currently stationed at the Division of Technical Development and Mission Support.

Q And what is your job with the United States Secret Service?

A I'm the deputy assistant director that would be in charge of the grounds of the White House, the Vice President, anything technical that has to do with protection.

Q Where were you -- what was your job prior to that?

A Prior to that, I was in the Government Public Affairs Department.

Q How long have you been working for the United States Secret Service?

A Approximately 31 years, sir.

Q Can you explain for the jurors what the primary missions of the Secret Service are?

A Sure. So the primary mission of the Secret Service, back in 1865, when we were created, was to combat counterfeit. At that time, about 30 percent of all the money in circulation was

counterfeit. Then, in 1901, after assassination, they gave Secret Service a jurisdiction to protect the President or any other of the protectees at this time. So we have a dual mission of protection and investigation.

Q Thank you.

Your investigative mission, has that expanded beyond counterfeiting?

A It has. In the mid-'80s, it expanded to more financial based, cyber, computer based.

Q And when you use the word "cyber," what do you mean by that?

A Any computer fraud, computer-aided investigations as it involves any financial institution or credit card.

Q So why did the Secret Service become involved in the investigation of cybercrime?

A With the passing of that law and the creation of electronic crimes task forces, that's one of the major investigations the Secret Service is involved in.

Q How long have you been stationed in Washington, D.C.?

A Approximately one year this time.

Q With your prior job just before this position, were you also in D.C.?

A I was.

Q Where were you stationed prior to moving to Washington, D.C.?

A Prior to Washington, D.C., I was the special agent in charge of the Honolulu office.
Q What does it mean to be the special agent in charge?
A So I would be in charge of all the investigations and protection in Honolulu and also the district, which stretches out over to -- covers Asia-Pacific, all the way over to Afghanistan, and then down under, Australia, New Zealand; so all of Asia-Pacific.
Q Did you have regional offices throughout that area?
A I did. I had offices in, at that time, Beijing, Hong Kong, Bangkok, Guam, and Sydney.
Q You said your geographic area for the Honolulu office included the entire Pacific region.
Does that involve working with foreign nations also?
A It does, yes, sir.
Q Does that include the Maldives?
A It did, sir.
Q How long did you serve as special agent in charge of the Honolulu field office?
A Approximately three years.
Q And where were you before that?
A Before that, I was in Washington, D.C., as the special agent in charge of the Technical Security Division.
Q And prior to that job, was there a point where you --
A Prior to that job, I spent three years as the special

agent in charge of the Seattle Field Office.
Q So that brings us back to this area.
A Yes.
Q What geographic region were you responsible for when you were the special agent in charge of the Seattle Field Office?
A So the Seattle Field Office, under it was the state of Washington, the state of Oregon, half of Idaho, Montana, and the state of Alaska.
Q And was your headquarters for that region here in Seattle?
A Yes. It was headquarters here, with satellites office in Portland, Spokane, Missoula, and Anchorage.
Q How many agents did you have employed here in Seattle?
A I probably had about 16 agents at that time.
Q Did you also have task force officers?
A We did. We had an electronic crimes task force, which was made up of local Secret Service agents and then law enforcement folks from outlying communities with local police.
Q Did those task force officers include any officers from the Seattle Police Department?
A It did, yes, sir.
Q I'd like to draw your attention to mid-2010, early 2011.
Are you familiar with the Seattle investigation of Defendant Roman Seleznev?
A I am, yes, sir.
Q Were you still working at the Seattle Field Office when

that investigation began?
A I was, yes, sir.
Q Who was the lead investigator on that case?
A So the lead investigator was Detective Dave Dunn, with the Seattle Police Department.
Q And do you recall approximately how far before your departure from Seattle that investigation began?
A So I think it started about eight or nine months before I departed, with the case out of the Spokane office, I think, was the first notification.
Q Okay. So for that last eight or nine months of your time in Seattle, were you responsible for supervising the electronic crimes task force and Detective Dunn?
A Yes, sir.
Q So did you know the general nature of the allegations and the investigation that was being conducted?
A I knew the general investigation, and Detective Dunn would refer to it as track2. That was the name I knew it.
Q Without going into specifics, what was the general nature of this investigation?
A That businesses were -- their servers were hacked, some malware was placed on it, wherein an individual from the outside was able to gain access into their servers and gain credit card numbers.
Q Were you directly involved in the investigation back in

2010/2011?

A Absolutely not.

Q After you left Seattle, did you become involved in the Roman Seleznev investigation again, sometime around the summer of 2014?

A Yes. I then became aware, with a phone call from our headquarters, saying that they --

MR. BROWNE: Objection, Your Honor.

THE COURT: Sustained.

BY MR. BARBOSA

Q What led to your involvement in the case in 2014?

A A call from my headquarters, sir.

Q What was the nature of your call?

MR. BROWNE: Objection.

THE WITNESS: The nature of the call was --

THE COURT: Not the content. You can't testify as to what someone else told you. You can testify as to, as a result of that communication, what took place.

So to that extent, the objection is sustained. Otherwise, please continue, Counsel.

MR. BARBOSA: Your Honor, I am offering this not for the truth of the matter asserted, clearly. It's to explain why he took steps that he took, without context as to what he was asked to do. And also, these are requests to do something, as opposed to assertions. I think these do come in for that

matter.

MR. BROWNE: First of all, you know, I object to the speaking objections, and I believe that was.

I think it's hearsay. I don't think it meets any of the exceptions to the hearsay rule. I renew my objection.

THE COURT: All right. The objection is noted.

Ladies and gentlemen of the jury, the testimony of the witness has been objected to on grounds that it's hearsay, in other words, that someone else told the witness something. That's properly sustained. However, the Court will overrule the objection, and the testimony the agent will give you will not be offered for the truth of the statement that was made to him, but only for the purpose of providing context, as an explanation of why he took certain actions or why he did certain things.

So with that, please continue, Counsel.

BY MR. BARBOSA

Q Why were you contacted?

A I was contacted by my office to render assistance in this investigation.

Q What type of assistance were you asked to provide?

A I was asked to provide assistance in locating Mr. Seleznev in the Maldives.

Q When you were contacted about him -- when was this, approximately?

A Late June 2014.
Q Okay. Was there a U.S. arrest warrant for Mr. Seleznev at that point?
A There was, sir.
Q Why were you asked to assist with him -- with locating him in the Maldives?
MR. BROWNE: Your Honor, I object. Why? That necessarily involves hearsay. I don't want to say any more.
THE COURT: Same ruling. Please continue.
BY MR. BARBOSA
Q Why were you asked -- were you asked to go to the Maldives?
A Yes. I was asked to go to the Maldives and supervise an operation with the location of Roman Seleznev.
Q Did you have reason to believe he was there?
A We did have reason to believe he was in the Maldives.
Q Okay. So why was your office contacted about this?
A My office was contacted -- as I said, the region which I supervised covered all the way over to Afghanistan. And with the Maldives being off the coast of India, that was under my jurisdiction.
Q So what were you asked to do in support of this trip to the Maldives?
A I was asked to coordinate with the embassy in Sri Lanka, which is the government -- official government entity that

covers the Maldives, and the Maldivian government to coordinate the location.

Q Okay. And were you expecting to take him into custody, Mr. Seleznev?

A With working with the Maldivian authorities.

Q Okay. If you were able to take Mr. Seleznev into custody, what were you supposed to do next? Where were you going to take him?

A To Guam, sir.

Q Why were you going to take him to Guam?

A It was the first U.S. territory that could be reached in flight from the Maldives.

Q And you mentioned that you were asked to coordinate with the embassy in Sri Lanka.

Who, specifically, were you coordinating with there, and who else was involved in the operation, from the U.S. government side?

A So from the U.S. government side was a Department of State special agent by the name of Mark Smith, who worked in the Sri Lanka Embassy.

Q Thank you.

Was there anybody else from the Secret Service involved?

A There was a special agent who worked in the Bangkok office, under my supervision. His name was Special Agent Dan Schwander.

Q Why was the State Department involved in this operation?
A As it was a diplomatic effort between the government of the Maldives and the Sri Lankan Embassy.
Q And did you personally eventually travel to the Maldives as part of this operation?
A I did, sir.
Q Was it typical for you, as a special agent in charge, to take part personally in an arrest operation?
A Not normally in an arrest operation, but they had asked me to go to finalize the plans and to supervise the operation.
Q So when did you leave Hawaii?
A I left Hawaii on July 2.
Q And is there a time difference between Honolulu and the Maldives?
A I think about 14 hours. I'm sorry. I'm not exactly sure.
Q Do you recall what day it was when you arrived in the Maldives?
A I arrived in the Maldives on July 4, in the afternoon.
Q How long did it take you to get there?
A I think it took me about 27, 28 hours of direct transit.
Q I'm going to show you, but not publish, what's been marked as Government's Exhibit 12.1, which is three pages.
Do you recognize that exhibit?
A It's not on the screen. Do I have to hit the power button?

Q It's not on the screen in front of you?
A Yes, it's on.
It appears to be an aerial photograph of what I consider Male, or the Maldives.
Q And does that fairly and accurately represent the islands that you traveled to in July of 2014?
A It does, sir.
MR. BARBOSA: Move to admit and publish, Your Honor.
THE COURT: The particular exhibit, just 12.1?
MR. BARBOSA: Yes --
MR. BROWNE: No objection, Your Honor.
MR. BARBOSA: -- just 12.1.
THE COURT: 12.1 is admitted.
(Exhibit 12.1 was admitted)
BY MR. BARBOSA
Q How big were these islands?
A Not very large, sir.
Q Had you ever been there before?
A I had not.
Q Geographically, can you explain where these islands are located?
A Sure. It's off the southern eastern tip of India, in the Indian Ocean.
Q When you arrived in the Maldives, were you carrying a weapon?

A I was not.
Q Do you typically carry a weapon on duty?
A I normally carry one on duty, but I normally do not travel commercially, to a foreign country, with a firearm.
Q I see.
So when you arrived in the Maldives, what did you do after getting there?
A After arriving there, I was transported via a police boat to the government compound on the island of Male, to meet with the Maldivian officials and police.
Q And did you also meet with your colleagues from the U.S. government?
A I did.
Q And where was the meeting with the Maldivian authorities?
A In their headquarters building, in the city of Male.
Q How long did you meet with them that day?
A I think we met with them for about two, two-and-a-half hours, best of my recollection.
Q Did you provide any information to the Maldivians about Mr. Seleznev?
A We did.
Q What type of information did you provide?
A We gave them a copy of the indictment from the Western District of Pennsylvania from -- dated back in 2011.
Q What did you do after that meeting -- sorry. Just a

follow-up question about the copy of the indictment.
Was that from the Western District of Washington?
A Yes. What did I say? I'm sorry.
Q I think you may have said "Pennsylvania."
A I'm sorry. I apologize.
Q Have you worked in a number of different locations?
A Yes, I have. I apologize.
Q What did you do after the meeting with the Maldivians?
A After the meeting, we departed their vehicle, went back to the hotel, which is on a little separate island, and just worked on our operational plan for the next morning.
Q What was the basics of your operational plan?
A The basics of our operational plan was that the Maldivian authorities were going to work with us to meet Mr. Roman Seleznev upon the arrival of his float plane from the hotel in which he was staying, then go from there to see if they could identify him properly by his passport, and then take him to what I would call the tourist police station, to talk to him.
Q Did you know when he was going to be leaving the Maldives?
A We had information that he was going to depart the Maldives on July 5.
Q Was that the next morning after you arrived?
A That was the next morning, sir, yes.
Q What happened the next morning, July 5?
A So July 5, early in the morning, probably 7:00 a.m., we

met with the Maldivian police counterparts, Mr. Schwander, and Mr. Mark Smith, from the State Department.

Q Approximately what time of morning was that?

A That was approximately 7:00/7:30 that we met up and discussed the final operational plan.

Q And we'll discuss that a little bit more in a moment.

What did you do after meeting up with the Maldivian law enforcement and your colleagues at 7:30?

A We divided up, and myself and the lead Maldivian police officer went to meet the arrival of the float plane that we had information that Roman Seleznev would be on.

Q You mentioned a final plan for the operation.

Who came up with this plan?

A The Secret Service, the State Department, and the Maldivian government.

Q I'm going to now show you what's been marked as Government's Exhibit 12.2, which is a series of photographs. And I'll move through these for you to review.

If you could just tell me if you recognize those.

A I do.

Q How do you recognize those?

A I was either in them or at that scene at the time, sir.

Q Were these all taken on July 5?

A They were.

Q Do these photographs fairly and accurately depict the

events that took place at the airport in the Maldives on July 5?

A They do, sir.

MR. BARBOSA: The government offers Exhibit 12.2 and requests permission to publish.

THE COURT: Any objection?

MR. BROWNE: I know, Your Honor, just let me look -- no objection, Your Honor. Thank you.

THE COURT: 12.2 is admitted.

(Exhibit 12.2 was admitted)

BY MR. BARBOSA

Q We're looking at Page 1 of Exhibit 12.2 now.

Who is this on the first page of Exhibit 12.2?

A That's myself and the supervisory Maldivian police arriving on the bus from the float plane to the general airport.

Q Okay. Is that the supervisor who came up with the plan?

A It was.

Q So what was the plan, specifically, for taking Mr. Seleznev into custody?

A The specific plan was to view him exit the bus, gather his luggage. He was going to then proceed to the departure area, in which you have to pass through tourist police or immigration police. And at that time, once identified, they were going to ask him to go to the tourist police, or immigration police

station, which is about a minute's walk away from the arrival area.

Q And what was the plan for you taking custody of Mr. Seleznev?

A The plan was for them to positively identify him. If that was done, we were told that the Maldivians were going to expel him, and we were going to take him into custody at that time.

Q What were you going to do after you took him into custody?

A We had a plane waiting there for him in which we were going to take him to Guam for processing.

Q Was that a commercial flight?

A It was not.

Q What was it?

A It was a private jet that we had arranged for, sir.

Q When you say "we"?

A Sorry, the United States Secret Service.

Q Was there any discussion about what to do with any luggage or other personal items he might be carrying?

A Yes. The plan called for Mr. Dan Schwander and the Maldivians to search the luggage, in the police station, while we were waiting.

Q This photograph on Page 1 of Exhibit 12.2, you explained, is after the float plane.

Where were Agents Schwander and Smith while you waited for the float pane to arrive?

A So when I was waiting with the Maldivians for the float plane, Special Agent Dan Schwander was actually in the tourist police station, and Special Agent Mark Smith was in the arrival area, where this picture would have been taken.
Q When did the float plane arrive, approximately?
A I think the float plane arrived just after 10:00 a.m.
Q And did you see Mr. Seleznev when it arrived?
A I did, sir.
Q How did you know what he looked like?
A From a copy of his photo that we had.
Q Where was he when you first saw him?
A Exiting the float plane.
Q Do you see Mr. Seleznev in the courtroom today?
A I do.
Q Could you identify him?
A Yes. Sitting in the shirt, white shirt, next to the attorney.
Q Was there anyone with him in the Maldives when you first saw him?
A There was. There was a small female child and an adult female.
Q What did Mr. Seleznev and his companions do after they got off the seaplane?
A After they got off the seaplane, they transited through an open area onto a transit bus.

Q What did you do?
A Followed him on the bus and sat on the first row.
Q Did this gentleman on -- in the photograph with you, on the first page of Exhibit 12.2, did he come with you?
A Yes. He sat across the aisle, in the other seat in the first row.
Q Turning to Page 2 of Exhibit 12.2, who is this in the photograph here?
A I know him as Roman Seleznev.
Q Where was this photograph taken?
A This was taken at the arrival of the transit bus from the float plane to the general airport.
Q When you saw him, was he carrying anything with him?
A Just a blue bag.
Q Is that the blue bag that is on his shoulder in this photograph?
A Yes, sir.
Q Where was his other luggage?
A His other luggage was being transported over. So the adult female and child departed off and went to the restroom, and Mr. Seleznev waited in that area where that picture was taken, for his luggage to arrive.

MR. BARBOSA: And, Your Honor, I forgot to ask to be sure that the record reflected that the witness did identify Mr. Seleznev in the courtroom.

THE COURT: Please continue.

BY MR. BARBOSA

Q When you got to the terminal, what did Mr. Seleznev do?

A He smoked a cigarette while waiting for the luggage to arrive.

Q What did you do?

A I just stayed in the area and watched.

Q So now turning to Page 3 of Exhibit 12.2, is that Mr. Seleznev?

A That is.

Q What were you doing at this point?

A Just observation.

Q And is that the same blue bag that you'd seen earlier?

A It is, sir.

Q Did you approach Mr. Seleznev at any point?

A Not at this time, no, sir.

Q Moving on to Page 4 of Exhibit 12.2, who is the woman in the photograph?

A That is the female that accompanied him off of the float plane and sat with him on the transit bus.

Q Did you contact her at any point during this?

A I did not, sir.

Q What happened after you see them here, outside the terminal?

A Approximately maybe three or four minutes later, their

luggage came, in which Mr. Seleznev picked it up, put it on a dolly, and then headed towards the entrance to the airport and met up back with the adult female and the female child.

Q What happened when they went into the entrance to the airport? What did you see?

A I observed them walking up to two Maldivian tourist police. They appeared to hand them their passport, at which time the tourist police escorted them to the police station.

Q Do you know approximately what time that was, how long it had taken from the float plane arrival to the tourist police beginning to escort them to the police station?

A I think they arrived at the entrance about 10:20 a.m.

Q I'll just ask to be careful of -- wait for the entire question, for the court reporter's convenience.

A Yes.

Q Where were you, Agent Schwander, and Agent Smith when the Maldivian police took them to the police office?

A Agent Schwander was inside the police office. Agent Mark Smith was directly behind him, behind Mr. Seleznev. And I was behind Mr. Smith.

Q Did you follow them into the police office?

A I did follow them into the police office, sir.

Q Turning to Page 5 of Exhibit 12.2, where was this photograph taken?

A That was taken inside the tourist police station.

Q Who is the gentleman in the green shirt?
A The gentleman in the green shirt is Special Agent Dan Schwander.
Q Who are the two gentlemen in the background?
A Those are the Maldivian tourist police.
Q Are they the same officers who brought him to the police office?
A They are.
Q Who is sitting down, looking up at Agent Schwander?
A Mr. Seleznev.
Q Were you in the room while this was going on?
A Yes. I was standing right behind that little knee wall, or half wall, in the picture.
Q Did Agent Schwander talk to Mr. Seleznev?
A He did, yes, sir.
Q What did he tell Mr. Seleznev?
A He identified --
MR. BROWNE: Objection, Your Honor.
THE COURT: Counsel?
MR. BARBOSA: Same -- it is not offered for the truth of the matter asserted.
THE COURT: All right. The objection is overruled. Please continue.
THE WITNESS: Special Agent Schwander identified himself as a Secret Service agent and identified Agent Mark

Smith as a State Department agent.

BY MR. BARBOSA

Q Agent Schwander has some papers in his hands.

Did he show these to Mr. Seleznev?

A Yes. He explained that he had a copy, and presented that copy to Mr. Seleznev, of the 2011 indictment from the Western District of Washington.

Q How did Mr. Seleznev react?

A The only thing I remember him saying is -- asking a question, if there was a extradition treaty with the Maldives.

Q How was Mr. Seleznev's demeanor?

A Calm.

Q What did you do after Agent Schwander presented the indictment to Mr. Seleznev?

A Agent Schwander and Agent Mark Smith and the Maldivian tourist police went through their luggage. I asked Mr. Seleznev to empty his pockets, and we placed those contents on the coffee table in the picture.

Q Did you review the contents of the blue computer bag that we had seen earlier?

A We did.

Q What was in that bag?

A A Sony tablet/laptop, a second phone, a second passport, some papers, cash, credit cards.

Q Let's talk a little bit about the Sony laptop.

How closely did you examine that laptop while you were still in the police station?
A I did not closely examine it while in the police station, sir.
Q Did you notice anything particular about it?
A Other than I had never seen a computer like that before. Other than that, no, sir.
Q What was unusual about it?
A It looked like a tablet, but appeared to be a laptop.
Q Did you turn it on?
A I did not.
Q Did you try to operate the computer in any way?
A Not in any manner, sir.
Q About how long did you look at it while you were there in the police office?
A Maybe ten seconds.
Q Did you count the cash or inventory any of the other items at this point?
A No, sir.
Q What did you do with the personal items that you found on Mr. Seleznev?
A Placed them back in the blue bag and kept them with me.
Q After you finished placing the items back in the bag and taking them, what happened next?
A The Maldivian tourist police escorted Mr. Seleznev,

Mr. Schwander, Mark Smith, and myself to a VIP lounge area, for processing the passports.

Q How long did the passport processing take?

A Probably ten minutes, 12 minutes.

Q Where did you go from there?

A From there, we were transported via a small bus out to the private plane.

Q Do you recall about what time you got on the airplane?

A I think maybe two or three minutes after 11:00.

Q And what time did you take off?

A 11:17, we were wheels up, sir.

Q About how much time had passed since you first saw Mr. Seleznev at the float plane dock and you took off for Guam?

A Approximately one hour.

Q I'm showing you what's been marked as Government's Exhibit 12.10 on the overhead. This is two photographs.

Do you recognize those photographs?

A I do, sir.

Q How do you recognize those?

A Those were the -- those are pictures of the inside of the plane, sir.

Q Do they fairly and accurately depict how things appeared on the flight to Guam on July 5?

A They do, sir.

MR. BARBOSA: Government offers Exhibit 12.10 and

asks permission to publish?

THE COURT: Any objection?

MR. BROWNE: No objection.

THE COURT: It's admitted. You may publish.

(Exhibit 12.10 was admitted)

BY MR. BARBOSA

Q Looking at Page 1 of Exhibit 12.10, can you describe what we're looking at here?

A Certainly, sir. You're looking at a photo from the rear of the plane, forward.

Q How long was the flight?

A The flight to Guam was approximately 11 hours.

Q What was the paperwork here on the table in the foreground?

A So that paper is our inventory -- evidence inventory forms. And that is Mr. Schwander, sitting at the table.

Q What are those evidence inventory forms for?

A For chain of custody for evidence, sir.

Q And what was displayed on the screen in front of Mr. Seleznev?

A That was the GPS routing from us, from the Maldives to Guam.

Q Turning to Page 2 of Exhibit 12.10, can you describe what we're looking at here?

A Yes, sir. That's a picture of probably about mid-plane,

looking towards the rear of the plane and the rear compartment, with Mr. Dan Schwander in the green shirt. And I was actually in the back of that with the evidence, sir.

Q And are these some of the same inventory sheets we see here on the table, on the right-hand side?

A Yes, sir.

Q So how did you go about doing the inventory of Mr. Seleznev's personal belongings?

A So what we did was, I took out everything in the blue bag and laid it from end to end. In that picture to the left is a couch/bed. I laid it out from right to left and by types of items so that we could inventory.

Q I'm showing you what's been marked as Government's Exhibit 12.4.

Do you recognize that?

A I do, sir.

Q How do you know that?

A It was a picture of the evidence while it was laid out.

Q Does that fairly and accurately represent what you just described?

A Yes, it does.

MR. BARBOSA: The government offers Exhibit 12.4.

MR. BROWNE: No objection.

THE COURT: It's admitted. You may publish.

MR. BARBOSA: Permission to publish?

THE COURT: You may.

(Exhibit 12.4 was admitted)

BY MR. BARBOSA

Q So what do we see here in this picture, in Exhibit 12.4?

A So from left to right, some various cords, connectors, transiting paperworks, his cigarettes, miscellaneous paperwork, receipts from airlines, four credit cards, two cell phones, an iPad, the Sony computer, two passports, Russian dollars and U.S. dollars.

Q Can you describe the inventory process, what type of information you record?

A Just make, model, serial numbers. If it's a credit card, credit card number, bank issuer, just details so you can later identify and keep a chain of custody of that item.

Q In regards to the laptop, did you have to open the computer or otherwise manipulate it to find the serial number?

A I believe the serial number was between the two pieces, so I believe we had to open it up to get the serial number off.

Q And we see some cash here in this photograph.

Did you count the cash?

A We did, sir.

Q How much cash was -- how much U.S. cash was he carrying?

A In excess of $7,200, U.S. cash, and I believe 128,000 in Russian.

Q I'd like to look at some of the items you see.

MR. BARBOSA: May I approach, Your Honor?

THE COURT: You may.

BY MR. BARBOSA

Q Can you take those items out and review them real quickly, and let me know if you recognize them?

A Yes, sir, I recognize them.

Q How do you recognize them?

A By the names on the cards and the inventory sheet that's stapled to the outside, sir.

MR. BARBOSA: Government offers Exhibit 12.5.

MR. BROWNE: Your Honor, may I just ask a question in voir dire?

THE COURT: Yes.

VOIR DIRE EXAMINATION

BY MR. BROWNE

Q Good morning, sir.

A Good morning, sir.

Q Are those the credit cards?

A Yes, sir, they are.

Q Is that all that's in there, is the credit cards?

A I believe that's all that's in here. That's all that's in here right now, sir.

MR. BROWNE: No objection, Your Honor.

THE COURT: 12.5 is admitted. You may publish.

(Exhibit 12.5 was admitted)

DIRECT EXAMINATION

BY MR. BARBOSA

Q So those are physical exhibits you had in your hand. I brought up a photograph.

Are those the same, in the photograph, that we're using to display for the jury?

A Yes, sir, they are.

Q Now I'm going to bring up Exhibits 12.6 and 12.7.

MR. BARBOSA: May I approach again, Your Honor?

THE COURT: You may.

BY MR. BARBOSA

Q Do you recognize those?

A I do, sir.

Q How do you recognize Exhibits 12.6 and 12.7?

A Again, by the items themselves, backed up by the inventory sheet.

Q Okay. Are Exhibits 12.6 and 12.7 in the same or substantially the same condition as when you seized them from Mr. Seleznev?

A They are, sir.

Q Are those the same passports that Mr. Seleznev presented to the Maldivian police officials?

A May I open?

Q Certainly.

A Yes, sir. One is the exact one presented to the Maldivian

authorities.

Q And the other one, what was that?

A Again, I would explain this as an internal document for Russia, rather than an external. It's almost like a driver's license.

Q Was that the one you found in his bag?

A This was the one in his bag, yes, sir.

MR. BARBOSA: The government offers Exhibits 12.6 and 12.7.

THE COURT: Counsel, are you offering just the individual exhibit or the subparts of 12.6? In other words, there's 12.6A, B, 12.7.

MR. BARBOSA: Sorry. Just 12.6. I'm going to go over the sub-exhibits, which are photographs and translations.

THE COURT: Just 12.6 and 12.7.

MR. BROWNE: We had a previously ruling from the Court on this. Subject to that ruling, we would make our standing objection.

THE COURT: Objection is overruled. 12.6 and 12.7 are admitted. You may publish.

(Exhibits 12.6 and 12.7 were admitted)

BY MR. BARBOSA

Q Did you also photograph or have somebody else photograph the passports?

A We did, sir.

Q I'm going to show you Exhibits 12.7A -- I'll bring them both up so you can look at them at the same time -- 12.6A, on the overhead.

In preparation for trial, did you go over these photographs to confirm?

A I did, sir.

Q Do you recognize these photographs?

A I do, sir.

Q Both series, in 12.7A and 12.6A?

A Yes, sir.

Q And are those accurate photographs of the passports -- the physical passports that you have there in your hand?

A Yes, sir.

MR. BARBOSA: Government offers 12.6A and 12.7A.

THE COURT: Any objection to 12.6A and 12.7A?

MR. BROWNE: Same.

THE COURT: The Court overrules those objections. 12.6A and 12.7A are admitted.

(Exhibits 12.6A and 12.7A were admitted)

BY MR. BARBOSA

Q And have these also been translated?

A Yes, sir, they have.

Q Have you seen those translations?

A I have seen copies of the translations, yes, sir.

Q Showing you 12.6B and 12.7B, do you recognize those?

A Yes, sir, I do.

MR. BARBOSA: The government offers these conditionally. We do expect the interpreter to testify as the next witness.

THE COURT: Subject to the conditional admission, Counsel, same objection?

MR. BROWNE: Well, actually, I have a different objection.

If they're just being proposed, at this point, as a foundation for the next witness, I don't have any problem. But I don't think it should be admitted until we have testimony from the translator.

THE COURT: All right. That will be sustained, Counsel. So they're marked for identification, but they're not admitted at this point in time. This is only a foundational question.

MR. BARBOSA: No publishing at this point, then?

THE COURT: No publishing at this point.

MR. BARBOSA: Fair enough.

BY MR. BARBOSA

Q Bringing up 12.7A, which has been admitted, on the screen in front of you, Page 21 -- and if you could turn to that in the original exhibit too, it's easier to read -- does that list the defendant's name?

A It does, sir.

Q In English?
A It does, sir.
Q And his date of birth, did you go over those?
A Yes. It says, "Given name: Seleznev, Roman," 7/23/1984 for date of birth, and then Passport Number 640410831.
Q Does it also include the issue date and the expiration date?
A Yes. Issue date would be December 31, 2009. Date of expiry, December 31, 2014, sir.
Q Did you also seize paper documents from Mr. Seleznev?
A Yes, sir, we did.
Q I'm showing counsel Exhibit 12.9. And I'll bring that up to you in just a moment.
THE COURT: Counsel, while you're doing that, members of the jury, if you'd like to stand and stretch right now, please take advantage of it.
MR. BARBOSA: May I approach?
THE COURT: Yes.
Please be seated.
BY MR. BARBOSA
Q If you could take a moment to look at the items in the bag marked Exhibit 12.9.
A May I open the bag, sir?
Q Absolutely.

Do you recognize those items?
A I do, sir.
Q How do you recognize them?
A These would be the items that we seized out of the blue bag, from Mr. Seleznev.
Q So they were in the blue bag when you seized them?
A They were, sir.
Q Are they in the same condition as when you seized them from Mr. Seleznev?
A Yes, sir.
MR. BARBOSA: Government offers Exhibit 12.9.
THE COURT: Any objection?
MR. BROWNE: No, Your Honor.
THE COURT: 12.9 is admitted.
(Exhibit 12.9 was admitted)
MR. BARBOSA: Permission to publish?
THE COURT: Granted.
BY MR. BARBOSA
Q I have scans of the same exhibits on the overhead in front of you now.
What did you find in terms of paper documents on Mr. Seleznev?
A Transit receipts from airlines, from airline reservations, purchase of tickets, and travel documentation, sir, along with a key card to a hotel in the Maldives.

Q Thank you.

Let's focus on the first page. And I know they may get out of order, as you have the physical ones, but I'll show you the first page on the overhead.

Where was this airline reservation sent to? What e-mail address?

A A mail.ru e-mail address. And it's R-O-M-A-R-I-O-G-R-O-1.

Q Moving through these documents, most of these are in Russian; is that correct?

A They are, sir.

Q Did you recognize any of the destinations listed in any of these -- sorry. Go ahead.

A Yes.

Q Where were they for?

A For Male.

Q Is that the airport where you took Mr. Seleznev into custody?

A Male is the airport in the Maldives, yes, sir.

Q You mentioned some other items that you found on him.

What else was there?

A Again, transit airline documents; receipt stubs from Vladivostok International Airport, in the name "Roman Seleznev"; and other transiting documents, sir.

Q Did you also find hotel keys?

A We did, sir.

Q What were those for?
A For the Atmosphere Hotel, in the Maldives.
Q Turning to Page 20, is that the hotel key you're referring to?
A That is, sir.
Q Were you familiar with that hotel?
A I am, sir.
Q How?
A It's a hotel that's in part of the archipelagos off of the island of Male.
Q I'm going to turn your attention to Page 19 of Exhibit 12.9.
What is this?
A I believe that's his customs for the arrival in the Maldives, sir.
Q Possibly departure?
A I'm sorry. The departure, June 21.
Q And this stamp, when was that? Was that his arrival?
A Yes. That's his arrival card into Male.
Q And at the bottom of this, is this signed?
A It is, sir.
Q Did the defendant indicate a passport number on there?
A He did, sir.
Q Did that match the passport that you seized?
A It does, sir.

Q I want to turn to the laptop computer you discussed a moment ago.

MR. BARBOSA: I'm going to show Exhibit 12.8 to counsel.

May I approach, Your Honor?

THE COURT: You may.

BY MR. BARBOSA

Q I've now handed you Government's Exhibit 12.8.

Do you recognize that, if you could take a look at it?

A I do, sir.

Q How do you recognize it?

A Again, from the computer and the log sheet that accompanies it, sir.

Q Is this the same laptop computer you seized from Mr. Seleznev?

A Yes, sir.

Q Where was it when you first saw it?

A In the blue bag that was carried by Mr. Seleznev.

Q And did you inventory the serial number from that laptop that is marked as Exhibit 12.8?

A Yes, sir.

Q Where is the serial number located on it?

A It's located in between the -- there's a service tag number.

Q Okay. Is this the same computer?

A Yes, it is, sir.
Q And is it the same or substantially the same condition as when you seized it?
A It is, sir.
MR. BARBOSA: The government offers Exhibit 12.8.
THE COURT: Any objection?
MR. BROWNE: Yes, Your Honor.
May I ask questions?
THE COURT: Yes.
MR. BROWNE: You know what I probably would rule on that objection [sic], but I will ask some questions.
THE COURT: You may.
MR. BROWNE: Should I stand here?
THE COURT: You can stand there, Counsel, as long as you keep your voice up.

VOIR DIRE EXAMINATION

BY MR. BROWNE
Q Hello, again.
A Hello, again, sir.
Q That's Exhibit 12.8; correct?
A I'm sorry, sir?
Q Exhibit 12.8; correct?
MR. BARBOSA: Does it have an exhibit sticker on it that says 12.8?
THE WITNESS: I do not see -- I see a 14-108 on it,

sir.

MR. BARBOSA: Maybe flip it over.

BY MR. BROWNE

Q I think it's on the back.

A I've got it. Yes, sir.

Q You've got it?

A Sorry.

Q Is it 12.8?

A It is, sir, 12.8.

Q Okay. And since you had that in your possession way back when, in the Maldives and on the airplane, which we'll talk about in a bit, it's been in many other hands; correct?

A Define "many," please, sir.

Q More than five?

A I don't know that for certain, sir.

Q In any event, it's been -- since you last saw it, it's been handled by other people; correct?

A Well, there's a log on the form that should carry forward with this item.

Q Okay. So is that a yes -- let's just stick with one person.

It's been handled by somebody more than you since it was seized from Mr. Seleznev; correct?

A Yes, sir.

Q Okay. And is there anything on Exhibit 12.8 that

identifies that you actually had possession of it? Are your initials, or anything like that, on there?

A On the computer itself, sir?

Q Yes.

A No, sir.

MR. BROWNE: Your Honor, the objection is, there needs to be a better foundation.

THE COURT: Counsel, I suspect that you're going to have other individuals cross-reference the same item?

MR. BARBOSA: Items from it, not the physical item. Well, they'll handle the physical item.

The witness has testified that it has the same serial number. The physical exhibit has been properly identified, I believe.

THE COURT: All right. The objection is noted. It's overruled. 12.8 is admitted.

(Exhibit 12.8 was admitted)

BY MR. BARBOSA

Q So can you show the --

MR. BARBOSA: May the witness display the laptop for the jurors now?

THE COURT: You may.

BY MR. BARBOSA

Q Can you show the jurors how you open that computer up?

A So it's -- I thought it was a laptop, but it can open up.

And then I don't know, actually, where the release is, so I don't want to pull it -- oh, there it is. So it actually has a built-in keyboard. So at first, I thought it was an iPad. And then after getting it on the airplane, noticed that it was more of a laptop.

MR. BROWNE: Agent, you're trailing off voice-wise. You need to use the microphone.

THE WITNESS: Sorry.

MR. BROWNE: Thank you.

BY MR. BARBOSA

Q When you inventoried the laptop computer that you're handling there, was it powered on or off?

A It -- initially, it appeared as it did now, with the screen being black.

Q Did that change at any point?

A It did when I placed it on the couch, in the previous exhibit.

Q Is that Exhibit 12.4, that was already admitted?

A Yes, sir.

Q Is that -- so in the kind of middle bottom, is that the same laptop that we're talking about?

A It is, sir.

Q So what happened when you placed it here on the couch?

A I believe I bumped it on the arm or the pillow to the left in that picture. And at that time, the computer went on.

Q And when you say "the computer went on," what did you see?
A The screen lit up, and it appeared to be -- I'll call it an abstract rainbow design appeared.
Q How long did the screen display?
A Probably about 60 seconds.
Q What did you do when you saw the screen turn on?
A I left it alone.
Q Did you try and turn it off?
A I did not.
Q Why not?
A A rule -- or a golden rule, I'll say, with evidence, or electronic evidence, is to leave it in the state that you take possession of it.
Q Did you write any reports about the screen coming on?
A I did not, sir.
Q Did you tell anyone about it having displayed?
A I did.
Q Who?
A I told Mr. Schwander, Special Agent Schwander. And I also told Special Agent Mike Fischlin, when I delivered the computer to the Seattle Field Office.
Q After you completed the inventory, what did you do with the computer? Where did you put it?
A I put it back in the blue bag.
Q Did you do anything to make sure the screen wouldn't come

on again?
A I did.
Q What did you do?
A I actually asked the flight attendant for a bottle of water. And I removed the cap, the plastic cap, from that bottle, and taped it over the button on the side that I believe I touched, that lit up the computer.
Q Could you show the jurors the button you were trying to cover up?
A So I believe it was the button on the side. I believe that was the one. I'm still not certain if that is. But I believe that's what I touched that lit the screen. So I put the cap of the bottle over it, asked the flight attendant for tape, and I put it over in an "X" pattern so that it wouldn't go on mistakenly while it was in the blue bag.
Q Are there other buttons on that computer that you've since found?
A There are. There's a window button on the front, a touch button.
Q Did you try and cover that one up?
A I did not.
Q Did you look to see if the laptop had any indications that it could be capable of accessing a cellular network?
A I did not, sir.
Q Did you look to see if it had a SIM card?

A I did not, sir.
Q Do you know what a SIM card is?
A I do, sir.
Q What is a SIM card?
A It's the device that allows either a computer or laptop to gain access to a wireless network for communication purposes.
Q So you didn't see whether it had one?
A I did not, sir.
Q Do you know what a Faraday bag is?
A I do, sir.
Q Did you place the laptop in a Faraday bag?
A I did not.
Q Why not?
A I did not have a Faraday bag with me, sir.
Q So after you've inventoried it, taped a bottle cap over the power button, what did you do with it after that?
A Placed it in the blue bag, placed it behind the seat in the airplane.
Q And did it stay there for the rest of the flight?
A It stayed there for the remainder of the flight, sir.
Q How long was that flight?
A Approximately 11 hours.
Q Did you or anyone else ever remove it from the bag during that flight?
A No, sir.

Q After you arrived in Guam, what did you do with all the physical evidence you seized?
A It stayed with me, sir.
Q How long were you in Guam?
A Forty-eight hours, maybe.
Q Do you recall what time of day it was when you arrived in Guam?
A We arrived 2:45 -- 2:45-ish a.m., on July 6.
Q What day of the week was that; do you remember? Was that on a weekend?
A I believe it was on a weekend, sir. I'm not certain.
Q The first business day you're in Guam, did you escort Mr. Seleznev to the courthouse for an initial appearance?
A Yes, on the 7th.
Q What did you do with the computer and other evidence while you were in that court?
A While I was in court, it was locked up in the United States Secret Service Field Office that was in a federal courthouse in Guam.
Q Same courthouse where Mr. Seleznev appeared?
A Yes.
Q Did you have an office in that building?
A Yes.
Q Why did you have an office in the Guam Field Office?
A I'm sorry. It was in a different federal -- I'm sorry,

sir. It's in a different field. The field office is located in a different building than the courthouse that Mr. Seleznev appeared.

Q I see. Okay.

A I'm sorry.

Q So where did you leave the computer when it wasn't in your custody?

A In the United States Secret Service Field Office.

Q Okay. And was that field office secured?

A It is, alarms, cameras, bulletproof glass, bulletproof doors. Yes, sir.

Q Did anyone else have access to that evidence or the laptop while it was outside of your presence?

A They did not. It's my office when I'm there in Guam, sir.

Q At some point while you were in Guam, did you have an agent with computer forensic experience look at the computer?

A We did. Agent Lam, from our Los Angeles Field Office.

Q Did you see whether he turned the computer on?

A He did not, sir.

Q And were you with him at all times when he looked at it?

A Yes.

Q Did he operate the computer in any way?

A He did not.

Q Did anyone try and manipulate the buttons or the screen or anything about the computer?

A No, sir.
Q How did the computer get back to Seattle?
A I hand-carried it from Guam to Seattle, sir.
Q When you say you hand-carried it, was it out of the bag or in the bag?
A In the blue bag, with the rest of the evidence.
Q Where was the bag while you traveled?
A With me. It was at my feet, in the airplane seat.
Q When did you arrive in Seattle?
A 5:00 a.m. on July 8.
Q How long had you been traveling at that point?
A Probably 20 hours.
Q So did you have the computer in your possession the entire time from basically when you seized it in the Maldives until you got to Seattle?
A Absolutely, sir.
Q What did you do with it when you got to Seattle?
A I landed at the airport approximately 5:00, 5:30 a.m. Was met by Special Agent Mike Fischlin. He transported me to the Seattle Field Office of the United States Secret Service.
Q And did you give it to him?
A Yes. We laid out all the evidence on the conference room table, and I turned it over to his possession.
Q Was that the extent of your handling of the computer until now?

A Yes.
Q You mentioned you also seized an iPhone from Mr. Seleznev. I'm going to show you Exhibit 12.8.
MR. BROWNE: Twelve-point what, Counsel? Eight?
MR. BARBOSA: Sorry. 12.8A.
MR. BROWNE: Okay. Thank you.
MR. BARBOSA: May I approach, Your Honor?
THE COURT: You may.
BY MR. BARBOSA
Q Can you take a look at 12.8A and tell me if you recognize that?
A Yes, sir.
Q How do you recognize that?
A I believe it's the iPhone that Mr. Seleznev had in his possession, that was inventoried.
Q Why do you believe it's the same iPhone?
A It's on the inventory sheets from the plane and then the Seattle Field Office, sir.
Q So it has the same serial number you recorded --
A Yes, sir.
Q -- during your inventory?
A Yes, sir.
Q Okay. Is that the same iPhone, then, that you seized from Mr. Seleznev in the Maldives?
A Yes. It's the iPhone that's in the picture, sir.

MR. BARBOSA: Government offers Exhibit 12.8A.

MR. BROWNE: No objection, Your Honor.

THE COURT: 12.8A is admitted.

(Exhibit 12.8A was admitted)

BY MR. BARBOSA

Q Did you also transport this to Seattle and turn it over to Agent Fischlin?

A I did, sir.

MR. BARBOSA: No further questions, Your Honor.

THE COURT: Cross examination?

MR. BROWNE: Do you want me to go ahead and start?

THE COURT: Yes.

CROSS EXAMINATION

BY MR. BROWNE

Q Good morning, sir.

A Good morning, sir.

Q So I'll just start with some questions about the beginning of your testimony; okay?

A Yes, sir.

Q You don't have any jurisdiction in the Maldives; right?

MR. BARBOSA: Objection, Your Honor.

THE COURT: That's sustained, Counsel.

BY MR. BROWNE

Q Did you say on direct examination that your jurisdiction --

MR. BARBOSA: Objection again, Your Honor.

THE COURT: Counsel, if it's in response to the question the government asked, the defense is entitled to ask follow-up questions. To that extent, the government's objection is overruled.

BY MR. BROWNE

Q You testified on direct that your jurisdiction -- that was the word you used -- extended to Afghanistan; correct?

A That's the word you say I used. It would be my area of operation, would be that of Southeast Asia, sir.

Q So that doesn't necessarily mean you have jurisdiction in someplace like the Maldives; right?

A No, sir.

Q Did you have a search warrant?

A I did not, sir.

Q Did Mr. Seleznev give you consent to take his items?

A No, sir, he did not.

Q You remember one of the other agents -- Mr. Seleznev saying to one of the other agents a question, "Is there an extradition treaty with the Maldives," something like that?

A Yes, sir, something like that.

Q To the best of your memory, that's what was said? I'm sorry. I talked over you.

A Yes. To the best of my memory, that's --

Q Was that answered?

A It was not answered, sir.
Q There was no extradition process.
A Not that I know of, sir.
Q Now, let's talk a little bit about -- because I'm sure everybody doesn't know what a Faraday bag is. I do. You do.
A Faraday bag is a device named after --
MR. BARBOSA: Objection, form of the question. He's describing what a Faraday bag is, as opposed to asking a question.
THE COURT: Let's ask a question, Counsel. Sustained.
MR. BROWNE: Sure.
BY MR. BROWNE
Q Is a Faraday bag named after somebody named Faraday?
A I don't have that knowledge, sir.
Q Okay. What is a Faraday bag?
A A Faraday bag is a -- usually a foil-like bag that allows you to put devices that have wireless access -- the wired bag, or the aluminum bag, the metal bag, blocks any of those receptions from getting to the device after placed in the bag.
Q And the importance of a Faraday bag is that if an electronic device has a SIM card in it, it would prevent wireless --
MR. BARBOSA: Objection, again, form of the question.
MR. BROWNE: The purpose of the bag?

THE COURT: It's overruled, Counsel. But be mindful not to testify in the form of the question.

MR. BROWNE: Of course not. Sorry, if I did.

BY MR. BROWNE

Q A Faraday bag would prevent wireless communication with whatever device was in it.

A Yes, sir.

Q And that's particularly important, obviously, if not only important, for electronic devices that have SIM cards.

A Yes, sir.

Q And do you still have the computer up there?

A I do, sir.

Q Okay. Now, did you know, at the time, there was a SIM card in there?

A I did not, sir.

Q Okay. Do you know that now?

A I do, sir.

Q Okay. Can you point -- because I know there's a little port on there. Can you point to the ladies and gentlemen of the jury where the SIM card port is on Exhibit --

A If I can find it again. I wasn't the one that identified it.

Q I can help you find it, if you can't.

A Yeah. I actually don't know where it is, and I think it may be covered.

Q Look on the back, sir.
A So I -- I'm not certain where it is, sir. I'm sorry.
MR. BROWNE: May I approach, Your Honor?
THE COURT: You may.
MR. BROWNE: May I take the exhibit, Your Honor?
THE COURT: You may.
MR. BROWNE: Your Honor, may I confer with Ms. Scanlan for a moment?
THE COURT: You may.
BY MR. BROWNE
Q Now, there are also Faraday boxes; are there not?
A There are, sir.
Q Okay. And are you a forensic expert on computers?
A I am not a forensic expert, no, sir.
Q And that wasn't a criticism. That's not your field of expertise.
A It is not, sir. I'm a supervisor.
Q But clearly you knew, when you went to the Maldives, that you were investigating an allegation of a cybercrime; correct?
A Yes, sir.
Q And cybercrimes normally always involve computers; right?
A Normally, sir.
Q But you did not bring a Faraday bag with you?
A I did not, sir. I had maybe two hours' notice that I was leaving for the Maldives.

Q Okay. And if an electronic device has a SIM card in it, and that device is turned on, it can communicate with outside sources; correct?
A While it was on the plane?
Q Yes.
A I don't know if that's possible, sir.
Q We'll have somebody else answer that question.
A Okay.
Q But when you -- you actually accidentally, I believe, turned it on; right?
A It came out of hibernation on the plane, after we were wheels-up.
Q But you actually bumped on something, and then the screen came on -- the screen saver came on; right?
A Yes. That generic rainbow, yes.
Q So you believe it was on?
A I would call that hibernation, not on, sir.
Q With the screen saver or without the screen saver?
A I would -- I would say a hibernation screen, sir.
Q Okay. But the reason you asked for the bottle cap to put over the button that you thought was the on-and-off button is, you were concerned that somebody might -- it might, on its own, turn on or turn off?
A Well, as I had spoke, I had never seen a Sony Vaio laptop of this nature. I wasn't sure what it was. I wasn't sure how

to turn it on, how to turn it off. So I put the bottle cap over what I believe made it go out of hibernation.

Q I'm -- I'm having trouble with that.

"Out of hibernation," what do you mean?

A Out of sleep mode.

Q Once again, we've established you're not an expert on computer forensics; right?

A Yes, sir.

Q All right. You get this computer. While you were on the airplane, there's some touching of it, in some way or another, and the screen lights up.

Can we go that far?

A Yes, sir.

Q You don't know what that means, whether that's on or hibernation. You don't know that; do you?

A No.

Q And in an exercise of caution, which makes perfect sense, you put the bottle cap over something you thought might be an on-and-off button.

A Yes, sir.

Q Am I right so far?

A Yes, sir.

MR. BROWNE: Okay. Excuse me, one moment, Your Honor.

May I, Your Honor?

THE COURT: Yes.

BY MR. BROWNE

Q I don't know how we can miss it, but apparently -- do you see that, the big arrow?

A Oh, yes.

Q If you actually push on that, there's a SIM card in there? You can go ahead and do that.

A Yes.

Q Okay. Would you point that out? Let me get out of the way. Would you point that out to the ladies and gentlemen of the jury?

A So there's a slot in the back, along this ridge.

Q And did you determine there was a SIM card in there?

A There is.

Q Okay. Now -- I think you can leave that there. Thank you, sir.

Were you the agent in charge of this case?

A Can you repeat that, please?

Q Were you the agent in charge of this case?

A At what time, sir? Sorry.

Q Well, let's say when you came back to Seattle. You brought the computer back to Seattle; right?

A Yes.

Q At that time, were you in charge of the case?

A No, sir.

Q Okay. Did you ever request that that SIM card be examined to determine what was on it?
A I didn't know there was a SIM card in there, sir, as I previously stated.
Q So I guess the answer is, no, you didn't do that.
A I did not know there was a SIM card in it, sir.
Q So you never requested, obviously -- it's an obvious question.
When the computer was in Guam, in the office that you've described, it was not in a Faraday bag either; was it?
A It was not, sir.
Q And this is a United States Secret Service office in Guam?
A Yes, sir.
Q And Guam, by the way, is a U.S. protectorate; right?
A I believe so.
Q So you do have jurisdiction in Guam.
A Yes, sir.
Q Did you inquire of other Secret Service agents or staff whether they had a Faraday bag?
A No, sir, I did not.
Q Were you concerned that if the computer was indeed on, it was communicating with other computers while it was in your office?
A At that point in time, sir, as I said, I did not know it had a SIM card in the computer.

THE COURT: Counsel, is this a convenient time to take the morning break?

MR. BROWNE: Sure.

THE COURT: Members of the jury, we'll take our morning recess. It is 10:30.

(Jury exits the courtroom)

THE COURT: Counsel, just for the benefit of counsel, so you always know, I will always ask, before we take a break, is there anything to take up before we take the recess? This is the proper time to take it, as opposed to having the jury come back when I come back and say, "Your Honor, there's a matter we want to take up."

So I'm asking now, counsel for the government, anything to take up?

MR. BARBOSA: No, Your Honor.

THE COURT: Counsel for the defense?

MR. BROWNE: No, Your Honor.

THE COURT: We'll be in recess.

(Recess)

(Jury enters the courtroom)

THE COURT: Counsel, you may continue your cross examination of the witness.

MR. BROWNE: Thank you, Your Honor.

BY MR. BROWNE

Q Hello, again.

A Hello, again, sir.
Q So Agent Lam, he's a Secret Service agent?
A Yes, sir.
Q And was the first contact you had with him in this case in Guam?
A Yes, sir.
Q Okay. And do you know -- I don't know the answer -- do you know whether Agent Lam is an expert on computer forensics?
A I don't know that, sir.
Q So, but from your testimony, I understand that Agent Lam did something with the computer when you were in Guam; right?
A I don't think he did anything with the computer.
Q What did you observe?
A I observed him more looking at the phones, sir.
Q Okay. I'm sorry. I thought you said in your direct testimony that he had some contact with the computer.
A He did. It was on the conference room table in my office, along with the other electronic items, sir.
Q Did he actually touch it?
A He may have, sir.
Q Okay. Now, that's an interesting computer in that the screen -- I can see why you thought it was a -- an iPad, or something, because the screen comes up and sits like this, right, on the computer?
A Well, I found out later, yes, sir.

Q And then so that's when the screen is visible, obviously, is when it's taken up and put like that; correct?
A So --
Q You can just show us. I don't think it's on now.
A The screen is visible -- this is the way -- in the state of which I observed it when I had taken possession of it from Mr. Seleznev.
Q Right.
A On the plane, when it was being inventoried and I had to try to locate a serial number for the form --
Q Right.
A -- what I did was exactly what I did here in court, is I kind of opened it -- I think you can kind of open it sideways and see the serial number. I did not fully extend -- I didn't know how to open it. So if you kind of just open it, you can see the serial number, and nothing else is visible, to include the SIM card.
Q Okay. Could you open it the way, though, if you wanted to use it? Could you just show us? Because it's an unusual --
A I think --
Q Or do you know how to do that?
A Well, I did when you brought it over.
Q Okay. Younger people know how to do that.
Could you just set it down for a second?
A Yes, sir.

Q So you did not see Agent Lam do that?
A I did not.
Q Okay. Does Agent Lam still work for the Secret Service, as far as you know?
A I believe so.
Q Okay. Now, we've identified one -- I think it's an iPhone, one cellular phone, Exhibit 12.8A; correct?
A Yes, sir, 12.8A.
Q Okay. Now, your testimony is that was taken from Mr. Seleznev's possession in the Maldives; correct?
A Yes, sir.
Q Okay. And there was another phone also; correct?
A Yes, sir. I believe a Samsung.
Q Okay. Now, was that phone on when you took it from Mr. Seleznev, or do you remember?
A The screen was not lit, sir.
Q Well, that doesn't mean whether it's on or not.
You don't know whether it was on or not?
A I do not.
Q Okay. And one of the purposes of a Faraday bag is to put something like an iPhone in the Faraday bag, which would prevent it from communicating also, correct, assuming there's a SIM card in it?
A Yes. Assuming there's a SIM card, a Faraday bag blocks communication via wireless.

Q Yeah. I think we've gone over that. Thank you.
Is that an iPhone? I think it is; right?
A I believe it is.
Q Does it have a little apple on the back?
A It does.
Q Did you have a search warrant to go into Mr. Seleznev's computer at any time?
A Did I?
Q Yes.
A No, sir.
Q Did you have a search warrant to go into Mr. Seleznev's phone at any time?
A No, sir.
Q You didn't even have a search warrant to take them into your custody; did you?
A No, sir.

MR. BROWNE: Thank you very much, sir.

THE WITNESS: You're welcome, sir.

MR. BROWNE: Thank you, Your Honor.

THE COURT: Redirect?

REDIRECT EXAMINATION

BY MR. BARBOSA

Q Did you need a search warrant to take those?
A Not to the best of my knowledge, sir.
Q Why not?

A The Maldivian authority turned over that equipment and evidence to us.
Q Did you see the SIM card that Mr. Browne found for you before today?
A I believe in the last court hearing, in this courtroom, it was identified, sir.
Q Okay. Was that in June?
A In June. Prior to that, no, sir.
Q And I should say, in June of 2016?
A Yes, sir.
Q So not at any time during the trip to the Maldives, your transport through Guam, or delivering it to Seattle?
MR. BROWNE: Your Honor, I'm going to object to the leading question.
THE COURT: It is leading, Counsel. Sustained.
BY MR. BARBOSA
Q Did you see it at any time during your trip to the Maldives?
A No, sir. I had never seen the computer fully extended to where that was visible.
Q Did you see it any time during your trip to Guam?
A Absolutely not.
Q Did you see it any time during your transport to Seattle?
A Absolutely not.
Q When was the first time you saw the SIM card?

A In court, in June of 2016.
Q Why couldn't you see it, again?
A It is not visible unless the computer is fully extended, which I did not do in the plane -- or excuse me. I did not need to do to get the serial number.
Q You mentioned you didn't have a search warrant to look through the computer or the iPhone; is that right?
A That's correct, sir.
Q So did you look through the computer or the iPhone?
A Absolutely not, sir.

MR. BARBOSA: No further questions, Your Honor.

THE COURT: Re-cross?

MR. BROWNE: No, Your Honor.

THE COURT: Any objection to this witness being excused, by the government?

MR. BARBOSA: No, Your Honor.

THE COURT: By the defense?

MR. BROWNE: No, Your Honor.

THE COURT: Thank you, sir. You're excused.

Counsel, please call your next witness.

THE WITNESS: Thank you, Your Honor.

MR. WILKINSON: The United States calls Andrei Medvedev.

THE COURT: Please step forward, sir.

THE CLERK: Please raise your right hand.

ANDREI MEDVEDEV, having been duly sworn, was examined and testified as follows:

THE CLERK: Have a seat.

If you could please state your first and last names, and spell both for the record.

THE WITNESS: Yes. My first name is Andrei, and my last name is Medvedev. And the spelling is A-N-D-R-E-I, M-E-D-V-E-D-E-V.

THE COURT: You may inquire.

MR. WILKINSON: Thank you, Your Honor.

DIRECT EXAMINATION

BY MR. WILKINSON

Q Good morning, sir.

A Good morning.

Q Can you tell us how you are presently employed?

A I am currently a freelance court interpreter.

Q How long have you been a court interpreter?

A I've been doing that since 2010.

Q And in what languages do you serve as a court interpreter?

A I do it in Russian and Ukranian languages.

Q Are you fluent in Russian?

A Yes, I am.

Q How did you become fluent in Russian?

A I grew up in Ukraine, in the city of Kiev, where Russian, I would say, is the most common spoken language.

Q And how long did you live in Kiev?
A Until I was 17.
Q And over that period of time, did you regularly speak Russian in your day-to-day life?
A Yes, I did. I also had my -- a part of my schooling in Russian.
Q And at some point in time, did you move to the United States?
A Yes, I did, when I was 17.
Q And can you describe your educational background in the United States?
A I attended and graduated from the University of Washington.
Q And what did you major in?
A That was in economics.
Q Have you obtained any certifications that allow you to interpret or translate in court?
A Yes, I have. I am Washington state certified court interpreter in the Russian language, and I'm also registered in the Ukranian language.
Q How many court proceedings have you interpreted or translated during your career?
A It would be hard to calculate to give you a precise number, but I would imagine it's at least hundreds, probably over a thousand.

Q Were you asked by the U.S. Attorney's Office to translate trial exhibits for this case?
A Yes, I was.
Q And what language were the original trial exhibits that you were translating them from?
A So they had been partly in Russian and partly in English.
Q And were you asked to translate them into English?
A Yes.
Q I'm calling up Exhibit 17.3.

Is Exhibit 17.3 a list of the exhibits that you worked with in this case?

A Yes.

MR. WILKINSON: Your Honor, the government would ask permission to display this list for demonstrative purposes. We won't be offering it into evidence.

THE COURT: Any objection, for demonstrative purposes only?

MR. BROWNE: No, Your Honor.

THE COURT: It's admitted for demonstrative purposes.

Just to make sure the jury understands what that means, "demonstrative" means it's admitted for purposes of serving as an aid to assist the witness in their testimony. A demonstrative exhibit will not be coming back to the jury room. So I want to make sure there's a clear distinction between the two.

Please continue, Counsel.

BY MR. WILKINSON

Q Okay. Just to remind the jury, is this a list of all the documents that you translated in this case?

A Yes.

Q And on the first column here, is that the trial exhibit number? There's a number there?

A I think so, yes.

Q Okay. And then there's another number next to that, which usually is the same number, but it has an "A" next to it.

Is that the Russian version of the translation -- excuse me -- the English version?

A Yes, it is.

Q And then is there a description column next to it?

A Yes.

Q And did you go through all of these exhibits, one by one?

A Yes, I did.

Q And did you either translate each one or confirm for each one that the English version was an accurate translation of the Russian original?

A That's right. I did.

Q How much time did you spend on this project?

A I think it was over 100 hours.

MR. WILKINSON: Your Honor, the government would move to conditionally admit all of the translations -- so it would

be the exhibit numbers in the second column there -- under Rule 104(b). And it will be conditional upon the admission of the corresponding Russian exhibit.

THE COURT: Any objection, Counsel?

MR. BROWNE: No.

THE COURT: All right. Those exhibits are all admitted as proposed by the government.

MR. BROWNE: Your Honor, I'm sorry. My understanding is they'd be admitted provisionally --

THE COURT: Conditional admit.

MR. BROWNE: Thank you.

BY MR. WILKINSON

Q There's a word here on -- it's about ten rows down, S-M-A-U-S. Do you see that word?

A Yes, I do.

Q Is that a word that you encountered, from time to time, as you reviewed all of these documents?

A Yes. I've seen it multiple times.

Q Can you pronounce the word?

A Smaus.

Q Is that a common Russian word?

A Not that I know of, no.

Q Have you ever heard it used in Russian?

A No.

Q And I want to ask you about one other word. And I'll

spell it for you, O-C-H-K-O, Ochko.
A Yes.
Q Is that a word that you encountered as you reviewed the Russian documents?
A Yes. I've seen it multiple times.
Q Okay. And is that a word that you have seen in Russian before?
A Yes.
Q And can you tell us what the meanings of it -- meaning or meanings --
A Well, it would have multiple meanings. It would have a meaning of a Russian blackjack, a card game. It could also mean a point, a game point. And it could also mean a butthole, and also a toilet seat.
MR. WILKINSON: No further questions for this witness.
THE COURT: Cross examination?
MR. BROWNE: No.
THE COURT: Any objection to this witness being excused, by the government?
Counsel?
MR. WILKINSON: Not from the government.
THE COURT: By the defense?
MR. BROWNE: No, Your Honor.
THE COURT: Thank you, sir. You may step down.

You're excused.

Counsel, your next witness?

MR. BARBOSA: Your Honor, the government calls Detective David Dunn.

THE COURT: Please step forward. Please step forward, sir.

THE CLERK: Please raise your right hand.

DAVID DUNN, having been duly sworn, was examined and testified as follows:

THE CLERK: Have a seat.

If you could please state your first and last names, and spell your last name for the record.

THE WITNESS: David Dunn, D-U-N-N.

THE COURT: You may inquire.

MR. BARBOSA: Thank you, Your Honor.

Before I proceed with my examination of this witness, I would offer Government's Exhibits 12.6B and 12.7B, which are the translations of the internal passport and the international passport, that Mr. Medvedev just confirmed. They were conditionally admitted under Agent Iacovetti.

THE COURT: Any objection to that, Counsel?

MR. BROWNE: Just the same objection, Your Honor.

THE COURT: All right. The objection is overruled. Conditional limitation has now been lifted.

(Exhibits 12.6B and 12.7B were admitted)

DIRECT EXAMINATION

BY MR. BARBOSA

Q Good morning, Mr. Dunn. Could you tell the jury where you're employed?

A I'm currently employed in two different places. The first is with a company called Kroll, and the second is with the Seattle Police Department.

Q Let's talk about your employment with Kroll.

What type of business does Kroll engage in?

A Kroll engages in a number of different businesses. They do large-scale e-discovery, so trolling through data for legal lawsuits; cyber incident response, so they do response to computer hacking and network intrusion cases. They do data recovery from failed hard drives. They have an identity theft notification service that they offer to companies, if they've been breached, to notify their clients, and a couple other smaller businesses.

Q What are your duties with Kroll?

A I'm the deputy chief information security officer. So I'm internal security for the company and all of its computers and servers. And I specifically manage the incident response team, the threat intelligence team, the vulnerability management group, security architecture, and threat research.

Q Where is Kroll located?

A Kroll is headquartered in New York City.

Q Do they have other offices?
A Yes.
Q Where?
A They have approximately 30 offices across the globe; in the U.S., primarily in Tennessee, Los Angeles, and southern Minnesota, Minneapolis; London, Germany, Norway, Sweden, Middle East, Asia.
Q Worldwide, it sounds like.
A Yes.
Q How long have you been with Kroll?
A I've been with Kroll since February of this year.
Q Where were you employed prior to joining Kroll in February?
A A company called FIS Global.
Q What is FIS Global?
A FIS Global is the world's largest financial services technology provider, which means they run or provide some sort of technology service to about 14,000 different banks and credit unions across the globe.
Q What type of technology services are those?
A So they offer credit card processing, core banking, fraud detection. Any service that a bank could conceivably need is something that could be purchased from FIS.
Q And what was your job with FIS?
A I was the vice president in charge of the global incident

response team and the threat intelligence team.

Q What did that involve?

A So I managed multiple teams, both located in the U.S. as well as overseas, to respond to any incidents within the Global FIS infrastructure, so tens of thousands of servers and the workstations for about 40,000 different employees. So I managed the teams that dealt with anything that went wrong with those devices from a security perspective. And I was also in charge of the threat intelligence team, which was actively looking for cyber threats that could impact the FIS business.

Q Okay. You've mentioned incident response in relation to both of your jobs.

What do you mean by "incident"?

A So when a cybersecurity event, be it a malware incident or a computer hack, occurs within the network or on a computer or server, a response is conducted by the incident response team. They look at the computer hard drive, they look at network connections, and determine what happened, how it happened, what's the scope. So is this the only device that was impacted, or were additional computers impacted? And then what type of information was potentially disclosed, if it was a bad actor that tried to steal data.

Q You also mentioned threat intelligence in relation to your FIS Global work.

What type of threat intelligence were you responsible for

collecting?

A So we were responsible for actively looking for cyber threats that could impact a business. For example, there was a time when computer hackers were attacking banks with what's called a "denial of service attack." And they would do that for either an extortion payment, or to cover up some other fraudulent activity that they were trying to do against the bank. So my team was responsible for tracking that, determining if the subjects were likely to attack us or one of our clients, and make sure that we were prepared for that incident.

Q You mentioned that FIS Global had a role in credit card payment processing.

Did you monitor threat intelligence related to credit card activity?

A Yes.

Q What type of threat intelligence?

A We specifically worked with the credit card brand, so Visa, MasterCard, American Express, and Discover, as well as other financial sector partners, to identify common points of purchase or places that we suspected had been breached and stolen cards could potentially be originating from. And then we also looked at banking malware, so what type of malware was impacting the consumer, banking computers, so that we could try to identify that malicious activity coming into our network, to

basically stop -- even if the system was infected, we could stop a wire transfer or bank transfer from going out.

Q How long did you work for FIS Global?

A I was with FIS for three years.

Q Has any of your work in the private sector, either with FIS Global or Kroll, touched upon this case?

A No.

Q So you mentioned another job, currently, that you have with the Seattle Police Department.

What is that job?

A So I served as a Seattle police officer for 12-and-a-half years, and I left in February of 2013. In August of 2014, I was brought back to the Seattle Police Department as a strategic adviser and a part-time detective to assist with this case, as well as others, to provide guidance and expertise. So I was given my badge and my gun back, and I just work as a part-time detective.

Q What did you -- you said you worked, I think, for 12 years for the Seattle Police Department.

When did you first start working there?

A I was hired by the Seattle Police Department in May of 2000.

Q When did you become a detective?

A I became a detective in April of 2006.

Q And at some point, did you begin working with the Secret

Service?
A Yes.
Q When was that?
A In October of 2006, I went from conducting forensic -- computer forensic investigations for the Seattle Police Department, and I was transferred to work on the U.S. Secret Service Electronic Crimes Task Force. So I began working out of the Secret Service Field Office in October of 2006.
Q Can you tell the jury what the Electronic Crimes Task Force is?
A Sure. So it's a task force model, meaning that multiple different agencies contribute to the task force. The Secret Service hosts it, meaning that they provide the infrastructure, the physical space, the desks, the phones, the computer connections. And then local agencies from Seattle, King County, Shoreline, Bellevue, all participate in the task force, and we use our sort of collective investigative ability to combat cybercrime that's impacting the Pacific Northwest.
Q What are the primary activities that the task force members engage in?
A So there's two primary activities. The first is to provide computer forensic support to our respective agencies. So we may do computer forensic investigations in support of a homicide case, or in support of a sexual assault case, or any other unit within the department. That's kind of one function.

And then the other function is to act as the primary investigators for computer hacking and network intrusion investigations.

Q How long were you originally with the -- does that also go by the acronym ECTF?

A Yes.

Q How long were you with the ECTF?

A I was with the ECTF from October of 2006 until I left the first time in February of 2013.

Q What's your educational background?

A I have a bachelor of arts from the Washington State University and an associate from Seattle Central Community College.

Q So turning your attention to the time period of 2010 through 2013 when you left -- originally left employment with SPD, were you involved in the investigation of the defendant, Roman Seleznev?

A Yes.

Q Without going into specific details at this point, could you describe, in general terms, the nature of your investigation?

A Sure. Beginning in May of 2010, I responded to a network intrusion at a restaurant in Coeur d'Alene, Idaho, that had been impacted by computer malware that was stealing credit card numbers. I began investigating that case through the summer,

including determining where the cards were being sold online. As it progressed through the fall of 2010, I identified additional victim businesses that were impacted by the same type of malware, located in the city of Seattle; obtained search warrants for e-mail accounts and other core process for records; and then ultimately was able to identify subjects involved -- hackers involved in the case, and ultimately obtained an indictment.

Q Did your investigation also involve conducting computer forensic examinations?

A Yes.

Q On different types of devices?

A Yes.

Q What types of devices did you examine?

A I examined computers, like typical PC. I examined computer servers, both within the victim businesses, as well as servers that had been located and were part of the infrastructure used as part of the network intrusion.

Q And you mentioned an indictment had been returned.

Was the investigation still open when you left the Electronic Crimes Task Force in 2013?

A Yes.

Q After you left in 2013, how did you end up back on the ECTF?

A In July of 2014, one indicted person was arrested. And in

preparation for trial, I was brought back to assist with that.

Q Before we go into the more intricate details of your investigation, I'd like to discuss some of your training and experience. And you've talked about both computer forensics examinations and investigating computer hacking and the network intrusions.

So let's start with investigating hacking and network intrusions. What type of training have you had to conduct these types of investigations?

A My training in computer forensics began in September of 2005. I attended approximately five weeks of specialized computer training. It was offered through Edmonds Community College, specifically for law enforcement, to teach computer forensics. That -- it was a part-time course, consisted of five total school weeks. And that carried me through the first quarter in 2006. That was my basic computer forensics training.

In April -- I'm sorry. In August -- late July and August of 2006, I was sent to the U.S. Secret Service basic computer evidence recovery school. So that was a five-week course that was held in Maryland and Virginia, for local law enforcement, to teach, again, the basic fundamentals of computer forensics and digital evidence collection.

Beyond that, I've attended numerous other computer forensic-related courses, specifically at the National Computer

Forensic Institute, in Hoover, Alabama. I've attended network intrusion training, which is a three-week course specifically to teach about investigating network intrusions. I've attended Macintosh forensics training. I attended advanced computer forensics training at the National Computer Forensics Institute. I've attended Linux forensics training, which is a specific type of operating system. I've attended point-of-sale intrusion training, specific to payment system breaches. I've received specific training on different computer forensic tools.

Q Does your training in relation to computer forensics and computer network intrusions -- are those similar, or are there different aspects of those two?

A They're similar in that they -- the topics are very closely related. The computer forensics is specifically related to obtaining computer drive evidence and examining that data, so examining the information that's specifically on the computer hard drives. The network intrusion aspect of it is -- more has to do with how data flows within the network, the connections that computers make with each other, and kind of building the bigger picture of an actual hacking event.

Q What type of network intrusion cases have you investigated?

A I've investigated a number of different types of network intrusion investigations, including other point-of-sale

investigations, other than this one. I've investigated credit card forums and credit card vending sites. I've investigated distributed denial of service attacks, so attacks that would prevent legitimate internet traffic from getting to a business. I've investigated banking malware-related cases.

Q Why does the Secret Service Electronic Crimes Task Force focus on financial cases such as point-of-sale?

A So the original mission of the Secret Service was to protect the financial sector of the U.S., so they -- that's why they have a counterfeiting mission. It was to sort of make sure that the currency was not devalued, that it remained safe. As part of that mission, it was expanded to include electronic payment instruments, and so the Secret Service continues to focus on maintaining the health and security of the banking sector.

Q Can you explain what a point-of-sale system is and what it consists of?

A Sure. So a point-of-sale, also known as a retail point-of-sale system, is the computer network that is located in many businesses across the world. And what it consists of is a computer terminal that the cashier or retail employee uses at the -- what's called the "front of the house," so the computer that a consumer and the retail person would interact with. And then typically, there is a back-of-house server, or a server that's located, like, in a manager's office.

When a consumer swipes their credit card or gives it to the employee to swipe the credit card, it's done at the point-of-sale terminal. And then that information is transmitted via computer network to the back-of-house server, which is in that back office, ultimately for processing.

Q Would it help you visualize this for the jury if you had a diagram of how this works?

A Yes.

Q I'm going to show you what's been marked as Government's Exhibit 17.5.

Would that help you describe things for the jurors?

A Sure.

Q Just a moment.

MR. BARBOSA: The government would offer Exhibit 17.5 as a demonstrative exhibit only.

THE COURT: Any objection, Counsel?

MS. SCANLAN: No objection.

THE COURT: 17.5 is admitted for demonstrative purposes only.

BY MR. BARBOSA

Q Using this diagram that is now on the screen for you and the jurors, can you explain what you just went over, in terms of how the point-of-sale system is typically set up?

A So in this diagram, we have four point-of-sale terminals. So in a typical retail establishment, you would have a number

of different checkout areas where a person can make their purchase, and there would be a point-of-sale terminal at each of those checkout areas.

To make your purchase, the card gets swiped. Typically, there's, like, a magnetic card reader that's attached to either the side, the top, or the bottom of the screen. The card gets swiped, and then that data gets transmitted via the network to the back-of-house server on the back of -- which is the device in the middle, the computer tower. The computer tower then communicates through a modem to the internet, and the credit card processing process takes place. Cards are -- the transaction is validated or approved or declined.

Q Is the data encrypted as it is traveling between these points at the business?

A Typically, within the business, the data is not encrypted. It's not encrypted until it gets transmitted out of the business.

Q And what would a system like this be typical for? Is this what you would see at a major retailer, with chains all over the country?

A So you could see this everywhere from a small retail establishment, with just one or two point-of-sale terminals, to your major retailers. Obviously, a major retailer would be more complex, because they would have more point-of-sale terminals. They might have two back-of-house servers to help

assist with the load. But the general network diagram would look something like this.

Q Approximately how many point-of-sale intrusion investigations have you participated in?

A Around 600.

Q And what types of businesses do you typically respond to, or did you typically respond to, in your work? Let's focus on your work with law enforcement and Secret Service.

A So typically, I responded to small franchise-type restaurants and small retail businesses.

Q I'm going to show you -- have you taken photographs of some of the systems that you've examined specifically as part of this case?

A Yes.

Q I'm going to show you on the overhead what's been marked as Government's Exhibit 1.14, which is a series of five photographs.

Do you recognize these?

A Yes.

Q How do you recognize these?

A These are images that I took during this investigation, at a restaurant located in Seattle.

Q And are those at various locations?

A Yes.

Q Do they all accurately reflect how the system appeared

when you went to examine them?
A Yes.
MR. BARBOSA: Government offers Exhibit 1.14.
MS. SCANLAN: No objection.
THE COURT: 1.14 is admitted.
(Exhibit 1.14 was admitted)
BY MR. BARBOSA
Q Turning to Page 1 of Exhibit 1.14, can you explain for the jurors what we're looking at? And you can reference the diagram.
A So these are two point-of-sale terminals that are located at MAD Pizza restaurant that was on Madison Avenue, in Seattle. So what you're looking at here are the touchscreen monitors that the cashier would use. On the right-hand side of the monitors, you can see, like, a black rectangle.
Q In this area that I've highlighted?
A Yes. That's the magnetic card reader. So that's where the card gets swiped. And from there, the data gets transmitted to the point-of-sale computer.
Q Turning to Page 2 of Exhibit 1.14, what do we see here?
A So these are a number of point-of-sale terminals, as well as the back-of-house server for that particular business. They didn't have a manager's office, so they were just kind of shoved underneath the main counter.
Q Do you recall where this was located at?

A This was also at the MAD Pizza on Madison Avenue, on First Hill.
Q Turning to Page 3, do you recognize this?
A Yes.
Q Where is this at?
A That's the third terminal at that same MAD Pizza location.
Q Moving on to Page 4, what's on this computer?
A That's the computer tower, covered in flour, underneath that screen at the MAD Pizza on First Hill.
Q Finally, Page 5, I don't know if this is even oriented correctly.
A This is upside down.
Q Okay. So what do we have here?
A So the picture is upside down. But if you look at the bottom of the picture, you see a metal rack. That metal rack is holding a computer tower, which is the point-of-sale system for the MAD Pizza that was in Madison Park. Then there's an old CRT monitor that was attached to it, as well. And then there's the keyboard that's just sitting on the ledge below it.
Q These setups that we've seen in Exhibit 1.14, are those typical of the type of systems you would see at smaller businesses?
A Yes.
Q How might a system like this get hacked?
A So most of these systems are installed by a third party.

So when you go to open up a business, you contract with a point-of-sale vendor who's going to sell you this point-of-sale system. Many of those vendors specialize in a specific type of merchant. So you may have one that specifically does recycling centers. You may have one that does pizza shops. You may have one that does rental -- tool rental places.

So you would find a person that sells a point-of-sale system for the type of business that you're in. And then you would pay them, and they would install -- either ship you or come out and install this system. Those systems are typically imaged identically. So a system located in Seattle, Washington, is going to have the same computer image as one in Portland, Oregon, or Los Angeles, California.

Inevitably, some of those systems will go down. They'll break. They're computers, and sometimes bad things happen. And the systems very often will have the ability for the vendor who sold the system to remotely connect to that system to fix that problem. So in the fast-serve restaurant business, approximately 70 percent of all transactions --

MS. SCANLAN: Your Honor, I object. This is a narrative.

THE COURT: It is a narrative, Counsel. Let's get back to questions.

BY MR. BARBOSA

Q Do small businesses like this typically have on-site IT

staff?
A No.
Q What would they do in order to fix problems that come up with their point-of-sale system?
A Call their vendor that they purchased it from.
Q How do the vendors provide that type of service?
A Remotely.
Q Can you explain how they would provide that type of service remotely?
A Sure. The vendor would have a remote application installed on the customer system, and they would connect remotely to that system, via the internet, to attempt to fix it.
Q Does that provide any method of intrusion that could be exploited by hackers?
A Yes.
Q How might a hacker exploit that method of access?
A Typically, those systems require just a username and password to gain access. So if you know the internet address for the system, and you know the IP address and the username and the password, you can log in remotely.
Q How could one go about identifying systems that have that remote access on them?
A There are tools that will allow somebody to scan large sections of the internet for specific computer ports that are

used for remote connections.
Q What is that scanning process known as?
A Just -- it's known as scanning. So that's --
Q Scanning for?
A Scanning for --
Q Port scanning?
A It's port scanning.
Q What is a port?
A So different computer applications that are connected to the internet talk on what's called a port. And a port tells the operating system what to do with the information that's coming into the computer. So Port 80 is the internet port, the unsecured internet port. So if information comes in on Port 80, your computer knows to give that information to your web browser. If it comes in on, say, Port 3389, it knows that's an attempt at a remote desktop connection, and to give that information to the remote desktop application. And there are many different ports that have many different uses.
Q That particular port, 3389, related to remote desktop applications, is that a port that you have seen used for remote servicing at point-of-sale systems?
A Yes.
Q And could one go about identifying open Port 3389 through this process of port scanning that you just talked about?
A Yes.

Q Okay. Can you describe how that port scanning process works and what it would provide to the hacker? How would somebody execute that type of a scan?

A So there are specific tools that will allow a computer hacker to scan wide ranges of the internet, so tens of thousands of unique IP addresses at a time. And they can specifically inquire to each computer, or each IP address, "Will you accept a connection on Port 3389?" And most computers will say no; right? Most of our consumer-level computers don't accept remote desktop connection. But some will. Some that are accessed remotely for various reasons will say, "Yes, I'm willing to accept a connection on Port 3389." So the first thing you do is the scan.

Q Once somebody finds those open ports, what would you do to access the remote program?

A So once you conducted the scan and you had one or more IP addresses that were willing to accept that connection, you could then use another tool to try a list of common usernames and common passwords to see if you are able to guess them correctly. It's called a dictionary attack.

Q If that dictionary attack is successful, what would the next step in the hacker's process be?

A So if your dictionary attack is successful, that means that you had a correct username and a correct password. You would then use the remote desktop application and connect

remotely to that system. And you would be presented with the desktop from the remote system.

Q What would this -- what level of control would this provide to the hacker in terms of the victim's point-of-sale system?

A Complete control.

Q Where would the hacker then need to install the malware? And I'm going to bring up Exhibit 17.5, again, for your reference.

A On the back-of-house server, or on one of the point-of-sale terminals.

Q And what would that -- what would a hacker typically install on these systems in order to steal credit card data?

A Some form of malicious software that was designed to look for and save credit card track information.

Q So as part of your work with the ECTF, as well as your private sector employment, have you become familiar with how credit cards work?

A Yes.

Q Have you had any training related to credit card payment processing?

A Yes.

Q And are you familiar with the types of data contained on a physical credit card?

A Yes.

Q Again, would it help you to demonstrate that for the jury if you had a demonstrative exhibit?
A Yes.
MR. BARBOSA: The government would offer Exhibit 17.1 as just a demonstrative exhibit.
THE COURT: Any objection?
MS. SCANLAN: Is it just on one page?
MR. BARBOSA: Let me double-check. I believe so. Yes.
MS. SCANLAN: No objection.
THE COURT: 17.1 is admitted for demonstrative purposes.
BY MR. BARBOSA
Q So let's look at the top half here, the front of a sample credit card.
Can you explain what type of information is contained on the face of the credit card?
A Sure. So you have the background of the credit card, which is the bank branding, tells you who issued the card. The large numbers, there's 16 of them. That's what's called the PAN, or the personal account number. The first six digits of the personal account number, so the 4000 12, is referred to as a bank identification number, or a BIN. That is a number that is unique to an individual financial institution. So every card issued by a certain bank will have a BIN that's issued to

that bank. So you would never have 4000 12 issued by both, say, Bank of America and Chase. Only one of them could issue those types of cards.

Q The first number, the "4," does that identify anything in particular?

A Sure. The first number indicates what type of card it is. Four is Visa. Five is MasterCard. Six is Discover. And three is American Express.

Q So looking at the back of the card, what is on the back of the card?

A So you have the -- a magnetic stripe, with what are called three tracks available.

Q Is that the black line?

A That's the black line.

Q Okay.

A Signature area; and then you'll have the card number and then what's called the card verification value, which is the "123" at the very end.

Q What is contained on the black stripe, the magnetic stripe?

A There's three pieces of information. There's Track 1, Track 2 and Track 3.

Q Let's go over those individually.

What's Track 1 contain?

A So Track 1 contains the personal account number, so that

16-digit number. There's what's called a separator, an equals sign. And then there's the card expiration date. There's what's called a card service code that tells where the card can be used geographically. There's a different card verification value, and then there's some additional discretionary data for the bank.

Q What does Track 2 carry?

A Track 2 carries the same information. It also includes the ability to encode the cardholder's name.

Q And finally, Track 3, is that used?

A Track 3 is rarely used. I've only seen Track 3 used on one occasion, and that's with Costco American Express. They use Track 3 to encode the Costco number, personal number for the shopper.

Q And then is the actual 16-digit credit card number written on the card, also, on the back?

A Yes.

Q What are the final three numbers?

A So that's the card verification value. That's that three-digit number that you input when you make an online purchase.

Q As to the magnetic stripe, how would you be able to read the data on that?

A So there are a number of different hardware tools that are available. They're called magnetic stripe readers. So that

magnetic stripe reader that's on the side of a point-of-sale terminal reads it and gives the information to the point-of-sale application. But you can also buy handheld magnetic stripe readers that you can plug into a computer and read the data that way, as well.

Q I'd like to show the witness Exhibit 17.2, just for demonstrative purposes.

THE COURT: Members of the jury, if you want to stand and stretch real quick.

Please be seated. Please continue, Counsel.

MR. BARBOSA: Thank you, Your Honor.

BY MR. BARBOSA

Q The courtroom deputy has provided you with Demonstrative Exhibit 17.2 in front of you.

Do you see that?

A Yes.

Q What is that?

A This is an MSR206 magnetic card reader/writer. So this can both read magnetic stripe data as well as encode magnetic stripe data onto a card.

Q And can you show that to the jurors?

A There's the slot where the card runs through. Inside that, there are magnetic reader heads that interact with the stripe. And it connects to a computer.

Q And does that require certain software to operate?

A Yes, it does.
Q How would you go about using one of those?
A So if you were to read a card or if you were to encode a card?
Q Let's start with read a card.
A So if you want to read a card, you would connect this device to a computer. And using special software, you could scan the card, and it would display what the track information from that card was.
Q How would you go about encoding a card?
A So using, again, specialized software, you would type in the information that you wanted encoded onto the card. And then once you would type in the information you wanted encoded, you would then swipe the magnetic card through the reader/writer, and it would encode that data on the card.
Q So turning back to Exhibit 17.1, our sample credit card for Mr. Smith, that data that you just talked about from the magnetic stripe, does that have any value to it?
A Yes.
Q Why is that information valuable?
A Because that information can be encoded on -- stolen information can be encoded on another card and used to make purchases.
Q Do you have any prior experience with how that stolen information or data is sold on the internet?

A Yes.
Q What type of experience?
A I've investigated credit card vending sites. I've investigated credit card forums. I've analyzed credit card forums and vending site database files. I've convicted other point-of-sale hackers.
Q Have you personally reviewed these types of credit card vending sites and credit card forums?
A Yes.
Q What is a carding forum?
A So a carding forum is an internet website where people engaged in credit card fraud, so the selling and purchasing of stolen card information and then the tactics and techniques to do that, will gather to discuss how they do things, as well as to advertise -- vendors will advertise their services and either sell directly from the site, or advertise websites where people can go to purchase the information.
Q Are carding forums open to the public?
A No.
Q How do you get to a carding forum?
A So to get to a carding forum, you'd have to know where the website is, and then you would have to register for access to the forum.
Q Have you done that before?
A Yes.

Q In an undercover capacity?
A Yes.
Q What does a carding forum typically look like when you visit it on the internet?
A Typically, it's pretty rudimentary, as far as websites go. It's usually just a screen with a list of different topics that people are currently discussing. You would click on a topic, and you could read about it. They'll sometimes have advertisements on the side or the top, for premium vendors who have paid for that advertising space.
Q If you join a carding forum, how do you identify yourself on the forum?
A Utilizing a nickname, also referred to as a "nic."
Q Let's talk about vending sites.
What is a vending site?
A A vending site is a website that's specifically devoted to the sale of stolen financial information.
Q Okay. And how do they differ from carding forums?
A So a vending site is going to be more sophisticated in the way that you interact with the site. A vending site will list what cards are for sale, and it's a more automated process. You would select the cards you want to purchase, you would make your payment to that site, and then that information would be delivered to you automatically; as opposed to a carding forum, where it's people commenting and talking about a specific

topic.
Q The data for sale on these sites, is this legitimate, authorized data?
A No.
Q Why doesn't law enforcement just shut these sites down?
A Many of the sites are hosted in countries where law enforcement is not able to get them taken down.
Q How do the buyers and sellers of the stolen credit card data, who participate in these carding forums and vending sites, how do they communicate, typically?
A They typically communicate via private messages within the carding site or via some type of messenger application. Oftentimes, they use one called ICQ.
Q What is ICQ?
A It's an internet chat program originally owned by AOL -- it's now owned by somebody else -- where you can register for an ICQ number. And utilizing your ICQ number, you can chat with people using the ICQ infrastructure.
Q And why is that a form of chat software that is used in the carding community; do you know?
A It's just a legacy, for lack of a better term, old-school chat application that's been around, and it's just widely accepted by the, sort of, hacking community.
Q Are there other forms of chat communications that hackers and carders have begun using more recently in your experience?

A Yes.
Q What types?
A The common one they use now is called Jabber. It's a more decentralized chat program. They'll also chat via mobile applications.
Q Do carders -- in your experience, do they also use more traditional forms of communication, such as e-mail?
A E-mail, Skype.
Q You mentioned that folks typically identify themselves using a nickname, or a nic.

What is -- based on your training and experience, is there any value in a nic?
A Yes.
Q Why is there value in a nic?
A There is inherent distrust when you're selling stolen information. So your nic is your reputation. And if you have a good reputation of selling quality stolen financial information, meaning that the buyers are able to use it and buy stolen laptops or buy whatever they need to buy, you're going to have a good reputation, and you're going to drive sales. If you have a bad reputation, that you rip people off, you're not going to drive sales. So your reputation helps drive sales.
Q Are there particular terms used in the carding community to describe items that are sold in the market?
A Yes.

Q What are some of the terms that you've come across, based on your --
A There's a number. So there's "dumps," "foals," "cards," "CDV." There's a bunch of different terms. And there's terms for everything. There's terms for the way things get paid for.
Q Let's talk about a few of those.
You mentioned "dumps." What is a "dump"?
A So a "dump" is a credit card that's being sold that contains the full track information.
Q The Track 2?
A Track 2, Track 1, or both.
Q Okay. Do you also come across the term "bases"?
A Yes.
Q What does that mean?
A So "base" is the database of cards. So you -- when somebody is vending stolen card numbers, they typically will sell them as a base. So they'll list 10,000 cards from a specific base. And that base will have a reputation, that, hey, these cards are really good, and we're getting a high validity off these cards. Or it will have a bad reputation, say, only 60 percent of these cards are working. So the base itself can have a reputation. And typically, that reputation degrades the older the base is.
Q You discussed the BIN number, or bank identification number, a little bit ago when we were looking at the sample

credit card number -- or credit card.

Is that BIN number -- is that used in the marketing of stolen credit card data?

A Yes.

Q How is it used?

A It helps the card purchasers buy cards that they feel will have a high likelihood of success.

Q How does that help them?

A So financial institutions have instituted things called velocity controls. And velocity controls prevent or flag transactions that are suspicious based on geography. So if I am located in Seattle, Washington, right now, and I buy lunch at a restaurant here, and in five minutes that exact same card number is being used in person at a Best Buy on Long Island to buy a MacBook, a velocity control is going to kick in and say, "There's no way that Dave Dunn made it from Seattle to New York in five minutes. That's a suspicious transaction." And they'll either decline it, or they may call me to see if it's a valid transaction. It's a velocity control.

Bad guys know this, and so they don't want to buy cards that are potentially located or being used simultaneously in a different area. So they'll try and buy cards near where they believe the card was issued so that it would look less suspicious for me to buy lunch now and then buy a laptop, say, at the Apple store at U-Village in 15 minutes.

Q How much does stolen credit card data cost, typically, on the internet?
A It depends on a lot of factors, including the database that it came from, the reputation of the hacker, and the type of card. But they can range -- for a good fresh card, the range can be $20 to $50 per card.
Q Okay. Let's move away from carding for a little bit.
As part of your work in both law enforcement and the private sector, have you developed experience with how the internet operates --
A Yes.
Q -- at its kind of core?
Can you explain, in general terms, how computers communicate over the internet?
A Yes. Computers communicate utilizing what are called IP addresses and domain name records. So IP addresses are the phone numbers of the internet, for lack of a better term. Every --
Q Let me stop you for a minute.
You've used that acronym a number of times. And I think you were talking about IP addresses in relation to port scanning; is that right?
A Yes.
Q What does "IP" stand for?
A Internet protocol.

Q And what does an internet protocol address look like?
A There are two versions, the most common version being IP Version 4, is four sets of numbers. So the numbers can be anywhere from zero to 255, separated by a dot. So, like, 101.101.101.101. That's an IP address. So each one of those sets that are separated by a period has to be between zero and 255.
Q How do computers use IP addresses to communicate across the internet?
A So every computer that is internet facing, meaning that it's exposed to the rest of the World Wide Web, has a unique IP address. And there are large indexes with the major internet service providers that know where those IP addresses are located. So if a computer in Seattle, Washington, wants to talk to a computer in Los Angeles, California, it works through internet IP records to find where the other computer's located, and then communicates with it.
Q Those internet indexes, are those available to the public for routing of communications?
A Yes.
Q Is that -- so how does that impact how the internet functions? What if those aren't available?
A The internet wouldn't function, because no computer would know how to get to another computer.
Q Are IP addresses useful to you in conducting your

investigations?
A Yes.
Q How are they useful?
A When we're investigating a case, and we're looking at activity that's being generated from a specific computer or a specific IP address, we can obtain records from the internet service provider that owns that IP address to determine where the computer is located and who may be operating it.
Q You mentioned, also, I believe, domain records.
What is a domain?
A So an IP address is the number. The domain is the web address. So if we take CNN.com, for example. CNN.com is the domain for the website CNN. That is mapped to an IP address. So what happens, when I tell my computer that I want to go to CNN.com, I make a request to what's called a domain name server. And I say, "Where is CNN.com?" And that domain server says, "CNN.com is over at that IP address, and here's how to get there." And then my computer connects.
Q Are those records also publicly available?
A Yes.
Q What would happen if they weren't publicly available?
A The internet wouldn't function.
Q You already went over ports. Why do computers use different ports to communicate?
A It enables separation of and security for the data that's

coming into the computer.

Q As part of your work in law enforcement in the private sector, you also developed experience with computer servers.

A Yes.

Q Can you explain what a server is and differentiate it from a typical personal computer that we might use?

A So a server is typically an enterprise or, like, a corporate-type device that serves a particular function. So you may have an e-mail server that serves up the e-mail for your work e-mail. You may have a web server that hosts a website that you're going to visit. You may have a file server at work that hosts all the work product that you and your team members are working on.

So a server has a specific function that it provides to a corporate or an enterprise-level network; as opposed to a personal computer, which is the device that we use to access those servers. So when we want to go on our personal computer to CNN, we actually access a web server that's hosting CNN's content.

Q Do servers also have their own IP addresses?

A Yes.

Q Does a person using a server need to be physically present in front of that server in order to utilize it?

A No.

Q Where are servers typically located?

A Servers are typically located in large warehouses. So you can either have what's called a co-location facility, where multiple businesses will have all of their servers together in the same warehouse. Or for some larger businesses, they may have their own server facilities.

Q So if your server is co-located with a number of other servers, does that give you access to everybody else's server?

A No.

Q What do you have access to when you are using or renting a server in a location like that?

A You have access to a console where you can remotely connect to that server and administer it.

Q When you say a console, do you mean a physical console?

A No. You get a virtual console. So from your desktop, you could access your server remotely.

Q How would one go about accessing that? What would you need to access that server?

A You would need a username, a password, and the IP address or domain for where that server was located.

Q How can a person go about obtaining access to a computer server, to a service like that?

A There are a number of companies that sell servers on demand. So if -- you can lease one for a period of hours, days, months.

Q Can a server be used for typical personal computing?

A It can, yes.
Q How?
A A server does have a web browser. It does -- you can install Microsoft Office on it, if you wanted to. So it does have the ability to function as a desktop computer, though it typically doesn't because the cost of a server is usually higher than a desktop computer.
Q In your experience investigating network intrusion cases and hacking, are servers used frequently?
A Yes.
Q How do you typically find them being used in these kind of crimes?
A Servers are used as part of the hacking scheme. So they can be used to stage hacking-related tools. For somebody, they can be used to launch scans, they can be used to launch attacks, they can be used to collect stolen information.
Q If you examine a server, what do you typically look for as part of your investigation?
A Typically, I would look for information related to what that server was being used for. So was it collecting stolen information? Was it hosting malicious software? Was it doing malicious activity related to scanning or brute forcing of passwords? Was the user using it as a personal computer, and is there information related to who that person is?
Q You testified that part of your work does involve

conducting computer forensic examinations.

What portion of your work involved doing the actual computer forensic examinations?

A From, like, a percentage basis?

Q Very rough guess on that.

A At the very beginning, I was almost a hundred percent focused on computer forensic investigations. Towards the end of my full-time law enforcement career, it was probably about 50/50, so halftime doing forensics and the rest of the time doing the network intrusion cases, although the forensics was often in support of my network intrusion cases.

Q So when you were conducting your network intrusion cases, did you typically do your own examinations?

A Yes.

Q Why is that?

A Because I knew the case better than anybody else, so I knew what to look for.

Q You've gone over some of your training that you received to become a computer forensics examiner, but do you have any certifications related to your work as a computer forensics examiner?

A Yes.

Q What certifications do you have?

A So I'm a certified computer forensic examiner through IACIS, which is the International Association of Computer

Investigation [sic] Specialists. It's a not-for-profit group that certifies forensics. I'm certified through Guide Software as an EnCase certified examiner, which is one of the software tools that I used for this investigation. I'm a Certified Information Security Systems [sic] Professional, or CISSP, which is a certification on general computer and information security. And I also have a number of expired certifications, including access data certified examiner, certified ethical hacker.

Q What is a certified ethical hacker?

A It's a training course and certification on identifying and investigating computer hacking activities, and what it looks like.

Q During the course of your career, has information in the field of computer forensics changed over time?

A Yes.

Q Do you receive any continuing education related to computer forensics?

A Yes.

Q How often?

A Now every couple years. During the -- my primary investigative years, I would receive usually two to three weeks of continuing education a year.

Q What types of computer systems have you been trained to examine?

A All flavors of the Windows operating system, from Windows 95 all the way through Windows 7. I've -- Windows Server, Macintosh, Linux, cell phones.

Q Approximately how many computer forensic examinations have you conducted in your career?

A Over a thousand.

Q So based on your training and experience, can you explain what it means, what are the basic steps of a computer forensic examination?

A So the initial step is to identify the computer evidence that needs to be seized and examined. So the first part is the collection of that evidence. And depending on what type of case it is, different collection methods could be used. But the first part is to create a forensically sound computer image, meaning you get a bit-for-bit copy of the computer hard drive.

Q What is a forensic -- sorry -- a forensic image?

A It means that you get an exact copy of the computer that you're looking at. Every bit is the same.

Q So why do you make a forensic image?

A Because you need that for the integrity of the investigation. You don't want anything to change. You want to be able to look at it exactly as it was, in that state.

Q Do you ever examine the actual original evidence?

A No.

Q Do you go about manipulating the computer and digging through it as if you were at the workstation?
A The only time you would do something like that would be, say, on a point-of-sale investigation, you would capture the computer memory. So you would have to interact with the computer for a short period of time to capture the computer memory, and then take your computer image.
Q So how do you go about making a forensic image?
A So depending on if you could power the computer down or not, if you can power it off, you would just turn the computer off; or if it was already off, you would remove the computer hard drive from the system. And then utilizing what's called a forensic write blocker, you would create an image of that drive utilizing specialized computer software. And that write blocker prevents writes, or changes, to the drives.
Q What software do you use to make the forensic image?
A Typically, I would use either FTK Imager or EnCase.
Q And is that forensic software that's used commonly in the field?
A Yes.
Q What do you do to make sure the image is the same as the original source evidence?
A So when you're making your computer forensic image, the software is creating a hash value, or a fingerprint of the data on that drive, as you're making your image. So once the image

has been made, once it's done, you have that fingerprint of the image. When you begin to examine the image, you hash that image again to make sure that that fingerprint is the same, that you're looking at exactly the same device. If one number on that entire hard drive changes, the fingerprint won't be the same.

Q After you obtain the forensic image, how do you go about examining the forensic image?

A So the forensic image is examined using specialized forensic software. In my case, I typically would use EnCase.

Q Again, is that software typically used in the field?

A Yes.

Q Does the forensic software that you use to conduct your examinations, does it show you the data the same way we see it, day-to-day, on our personal computers?

A No.

Q How does it display the information?

A It displays the information in lists of files. So it will give you a tree structure showing the folders and how they fit within that tree structure. And then you can view it many different ways. You can look at every file. You can look at specific files.

Q I brought up an exhibit. Would it help to show a sample screen from your software?

A Yes.

MR. BARBOSA: Okay. The government offers Exhibit 17.8 for demonstrative purposes. This is not specific to the case.

THE COURT: Any objection?

MS. SCANLAN: No objection.

THE COURT: It's admitted for demonstrative purposes only.

Counsel, it's almost 12:00, so let's finish this one area of examination.

BY MR. BARBOSA

Q What are we looking at here, on Exhibit 17.8?

A This is the main screen on EnCase. On the left-hand side you see the tree. So you see the disk image name is at the very top, TDurden. And then we're looking at the "C" drive, or the primary operating system drive. And this shows all the folders that are directly off of the "C" drive, so the program files, Windows, the user accounts.

The next pane over, where we just have that one line, the TDurden line, if you were to click on any one of these folders, it would list out all of the files that were located in that folder and any of its sub-folders.

Q And what is the field down here for?

A So depending on what you're looking at, say it was a Word document, you could view what the contents of the Word document are. If it was any other file, you could look at the actual

computer code for that file. So that can be used a number of different ways.

THE COURT: Members of the jury, it's 12:00. We'll take our break.

Please rise.

(Jury exits the courtroom)

THE COURT: Counsel for the government, anything to take up?

MR. BARBOSA: No, Your Honor.

THE COURT: Defense?

MR. BROWNE: No, Your Honor.

THE COURT: Have a good lunch.

(Recess)

THE COURT: Counsel, I wanted to bring a matter to your attention that was brought to the Court's in-court deputy. Apparently, Juror Number 5 just realized that he's had some familiarity -- or he does have some familiarity with one of the alleged victims in this case. And I believe it's --

THE CLERK: Village Pizza, in Anacortes.

THE COURT: Village Pizza, in Anacortes. And apparently, it didn't dawn on him yesterday, as we were going through this process, that, apparently, it's down the street in from his family's business, that he's familiar with, and that there are employees that he's familiar with that work in the MAD Pizza facility. And he wanted to bring that to the Court's

attention.

I have not had any communication, obviously, with that juror. The only information we have right now is what I've shared with you that was provided to the in-court deputy.

I think the proper thing to do with this information is to bring Juror Number 5 out and conduct additional voir dire examination of him to the extent of if that would affect his ability to be fair and impartial, if he had any discussions with anybody about the nature and scope of the investigation, and if he could avoid having any further communications with anyone there, or has anyone had any inquiries with him.

Let me hear from the government regarding the Court's proposal.

MR. BARBOSA: I think that sounds appropriate, Your Honor.

THE COURT: Counsel for the defense?

MS. SCANLAN: We agree.

THE COURT: All right. Bring him out.

MR. BARBOSA: Should the witness stay on the stand?

THE COURT: Actually, the witness should leave.

Sir, if you'd step down?

THE WITNESS: Yes, Your Honor.

(Juror Number 5 enters the courtroom)

THE COURT: Good afternoon, Juror Number 5.

You've shared some information with the in-court deputy.

And first of all, I want to tell you, you did exactly what the Court would expect you to do. As I mentioned yesterday during the course of voir dire, sometimes when we get into a trial, or sometimes there's conversations, then all of a sudden a light comes on, and you realize there's more information in your mind or in your memory than you perhaps recalled immediately. And so sharing information that you shared with the deputy is exactly what we would expect you to do. So you haven't done anything wrong, for starters.

Now, if you could share with the parties exactly what you shared with the in-court deputy, that would be helpful.

JUROR #5: Yeah. So I didn't catch earlier on that the Village Pizza was in Anacortes, which is actually where I'm from. And my family business is just a few businesses down. So I've actually met the owners. My parents know the owners pretty well, also. So I just didn't know if that had any implication.

THE COURT: And when you say your parents know, how about your relationship with the owners of that business?

JUROR #5: I've met them, but that's about it.

THE COURT: Have you had any conversations with them?

JUROR #5: No, not for a few years.

THE COURT: What's your best recollection of how long it's been since the last time you had communication?

JUROR #5: Probably in 2014, I would say.

THE COURT: And what types of things would you discuss when you would have conversation with them?

JUROR #5: We were just at a chamber of commerce meeting for businesses in Anacortes.

THE COURT: There wasn't any discussion about any of the activities that have been referenced so far in this case; have there?

JUROR #5: No.

THE COURT: The biggest concern the Court has is what impact that might have upon your ability to be fair and impartial.

Does the fact that your family knows the owner, or the fact that you grew up in Anacortes, would that affect your ability to be fair and impartial in your deliberations or consideration of the evidence in this proceeding?

JUROR #5: No.

THE COURT: And do you have any reservations or hesitation about that?

JUROR #5: I do not.

THE COURT: Would that take away from the responsibility or requirement that the government has to prove their case beyond a reasonable doubt?

JUROR #5: No.

THE COURT: If they failed to do that, would you have any difficulty returning a verdict of not guilty?

JUROR #5: No.

THE COURT: And has anyone contacted you from Anacortes, either family, friends, relatives about the nature of this case?

JUROR #5: They have not, no.

THE COURT: Have you had any discussion or communication with anyone about this type of activity taking place in the Anacortes community or any particular businesses?

JUROR #5: No, I have not.

THE COURT: Okay. I'll let the government ask follow-up questions.

MR. BARBOSA: No questions, Your Honor.

THE COURT: Counsel for the defense, follow-up questions?

MS. SCANLAN: No, Your Honor.

THE COURT: Okay. Juror Number 5, I specifically direct -- I'm going to confer with counsel. But I want to make sure that you not discuss what you shared with the Court with the other jurors. And if you go back in the jury room and someone asks you what happened, tell them to ask the judge. And I'm sure that they're not going to do that. Because they don't need to know what we discussed. But just tell them you're under court order not to discuss why I brought you out here.

JUROR #5: Okay. I understand.

THE COURT: Thank you, sir.

JUROR #5: You're welcome.

(Juror Number 5 exits the courtroom)

THE COURT: Counsel for the government, anything to take up regarding Juror Number 5?

MR. BARBOSA: No, Your Honor.

THE COURT: Defense?

MS. SCANLAN: No, Your Honor.

THE COURT: Okay. Let's bring the full jury in. Counsel, have your witness return to the witness stand.

(Jury enters the courtroom)

THE COURT: Counsel for the government, you may continue your direct examination of the witness.

MR. BARBOSA: Thank you, Your Honor.

BY MR. BARBOSA

Q When we broke for lunch, you were testifying about your computer forensics examination experience and the actual process of conducting a computer forensic exam. I'd like to talk some more about making the forensic image.

You referenced taking the hard drive out of the computer. Are there any instances where you don't take the hard drive out of the computer in order to conduct -- to make a forensic image?

A Yes.

Q When would you do that?

A So in instances with server operating systems, you will oftentimes image those live, a production server, so they're in use at that time. And a business can't afford for that server to go down, so you'll make what's called a live image. So you make that bit-for-bit copy of the server while it's up and running.

In instances where you're concerned that encryption may be involved, you would make a live image of the device, the concern being that if the power was removed from the hard drive, it would be encrypted. And without the encryption password or key, you wouldn't be able to gain access to the device again.

Q How would this live imaging process help you in terms of getting around encryption?

A So if you have a machine that's live, and you can access the desktop, you can utilize forensic tools to make that live image before the encryption is applied when the device is powered off.

Q You referred to servers, also, and businesses.

Have you conducted these types of live examinations?

A Yes.

Q And has that included point-of-sale intrusion investigations?

A Yes.

Q What about other computers, non-servers, personal

computers? Have you done live examinations of personal computers?

A I've done live examinations of personal computers. And another reason would be if you want to capture memory. The running processes on a system, you have to do that live, as well.

Q How do you conduct the write-blocking process in those instances?

A You're not able to write-block the drive, because it's currently up, the operating system is functioning. So the way that you address that is you use sterilized media, meaning that you take a completely clean and wiped hard drive with you, you bring your known and trusted tools with you, and that's it. Nothing else touches the machine that you're going to be imaging, with the exception of your clean hard drive and your forensic tools.

Q So back to the forensic image, you discussed the hash value and how that helps you assure the integrity.

Can you explain again, what is a hash value?

A So a hash value is basically a math algorithm that is run against the data. And at the -- once the algorithm has been run against the entirety of the data, you come up with a unique fingerprint; or it's a long string of numbers and letters that are unique to that specific set of data.

Q So do you conduct a hash value for both the original

source and the copy you've made?
A Correct.
Q Is that what you compare to each other?
A Yes.
Q Moving on to reviewing the forensic image, we had just started talking about Exhibit 17.8, the demonstrative example of your EnCase forensic tool. And you discussed a few of these areas here.

Can you discuss, in general, what else this tool allows you to do when conducting your examination?
A Sure. You can do keyword searches across the entirety of the drive for specific words that you want to look for. You can write what are called "expressions" to look for patterns. So you could look for a credit card track data pattern, because they have a consistent pattern to them. You can sort and look at just all of the pictures on the computer. You could look at just events that occurred during a specific time frame.
Q I'll ask a few questions in there.

So what parts of this EnCase forensic tool that we're looking at would assist you in conducting some of these exams?
A At the top there's a condition tab that would allow you to set a condition. So, for example, you could set a condition to look for just executable files, just programs.
Q Why would you look for that type of file?
A If you were trying to narrow down certain applications or

malware that might be present on the system, you would just want to look at the executables.

Q You mentioned timelines, also. Is that one of the features here?

A Yes.

Q What would you use the timeline feature for?

A When you're examining a machine, you may find a particular piece of malware that was placed on the computer at a certain date and time. And you can use the timeline function to view other activity that occurred on that drive at that same time, so to help you determine how the hack may have occurred, other files that may have been placed on the drive, files that may have been taken off or deleted.

Q What are the time stamps that you use to base that timeline from?

A The timelines come from the master file table, which is a part of the Windows operating system.

Q And what does the master file table tell you?

A It tells you a lot of information about the actual file, so when the file was created, when it was last written, when it was last accessed, if it's been deleted. There are a number of different things that it can tell you, where the file is currently stored on the drive.

Q Do you rely more heavily on some of the dates in the master file table than others?

A Yes.
Q Which dates do you rely on?
A The file created and the last written time are the most -- are the ones that I rely on the most.
Q Why are those the ones you rely on the most?
A The last accessed file time can be changed by automatic processes. For example, an antivirus scan against the drive can change an access time, because the file was accessed for the antivirus scan to run. It's not indicative that the file was touched by a user, but more of an automated process.
Q What are the other dates?
A The other dates have to do with when a file was actually manipulated. So if a file was last written to, say, a Word document, then that means somebody was actually typing on that document or making some form of change to it.
Q Generally speaking, what do you look for when you're conducting a computer forensic examination?
A Evidence of the crime and the information listed in the warrant. If there's a warrant or if there's consent, information related to the incident I'm investigating.
Q Do you look for information related to who was using the computer?
A Yes.
Q How do you go about looking for that type of information?
A It depends on if it's the victim computer or belongs to

somebody that I'm investigating. But you would look at files that the user created. You would look at internet history that was conducted with the device; pictures that may be stored on the device; data that may have been deleted, previously stored on the device.

Q You mentioned internet history. What types of internet history do you look for in relation to identifying who's using the device?

A People that may be accessing personal e-mail accounts, making online purchases, making travel reservations, any activity that could lead to information regarding the user.

Q Do you look for communications, or evidence of communications, when you're conducting your computer forensic exams?

A Yes.

Q What type of communications do you look for?

A E-mail, instant messaging logs, chat logs.

Q When conducting a point-of-sale hacking investigation, are there particular items that you look for?

A Yes.

Q What?

A Specifically, I'm looking for the type of malware that's located on the system, the date and time that the system was infected, information related to how the system became infected, any information related to the behavior of the

malware once it was installed on the system.
Q Do you look for credit cards?
A We do.
Q Do you have any particular tools to look specifically for credit cards?
A There are tools to look specifically for credit cards. I have an expression that I've written that finds them for me.
Q And when you say an "expression" that you've written --
A It's a computer script that I have that specifically looks for the credit card patterns.
Q This is a tool that you created?
A Yes.
Q What is the role of a search warrant in conducting a computer forensic exam?
A A search warrant gives the examiner authorization to examine the device.
Q So let's turn to the specifics of your investigation in this case. I'd like to draw your attention to May of 2010.
Were you asked to examine a computer system in Coeur d'Alene, Idaho?
A Yes, I was.
Q How did this come to your attention?
A I received a call from the Secret Service Spokane office. They had identified a likely business that had been hacked. And they didn't have the forensic resources available in

Spokane to deal with the intrusion, so they called me and asked if I'd be willing to travel from Seattle and help them with their investigation.

Q How is a business identified as a potential point-of-sale compromise?

A Through the financial institutions, they monitor fraud transactions that are occurring on their client cards. And they identify what are called common points of purchase.

Q What does it mean to identify common points of purchase?

A So they take all the fraud transactions that are occurring during a certain time frame, and they look to try to determine if there's a common business that all of those cardholders went to that might indicate that that business had been breached.

Q So did you go to Coeur d'Alene?

A Yes, I did.

Q What did you do -- what was the business name? I can't remember.

A Schlotzky's Deli.

Q And did you go to Schlotzky's?

A Yes.

Q What did you do when you visited Schlotzky's Deli in Coeur d'Alene?

A I first obtained consent from the owner to image the computer systems at his business. And then I proceeded to capture memory, as well as take live forensic images of the

back-of-house server, as well as the point-of-sale terminals in the business.

Q How did you go about conducting that live exam and capturing the memory?

A So utilizing sterilized media, so a clean hard drive in an external case and a forensic CD that had my tools on it, I inserted the CD. The first thing I did was run a program to capture the memory from the devices. Once I captured the memory, I then ran FTK Imager, which is a program you can run off the disk to create an image of the hard drive and save it to the external drive that I had brought.

Q Did you look at any of the evidence while you were still there?

A I waited until I got to the field office about an hour later.

Q What did you learn?

A That there was malware running, on a number of the systems there, that was stealing credit card information.

Q Did you look to see whether that system at Schlotzky's Deli had any connections outside of their network?

A Yes, I did.

Q How did you do that?

A I captured RAM, which is a type of memory on the system. And I used a tool called Volatility to look for connections from the system to external IP addresses.

Q What did you find?
A I found that there was a connection to an IP address that was in Russia.
Q How were you able to determine that that IP address was in Russia?
A Utilizing what's called a "Whois Lookup," which is synonomous to a phone book for IP addresses, I was able to determine that the IP address belonged to an internet service provider in Russia.
Q Based on your training and experience, did that lead to any conclusions, in your mind, about the Schlotzky's Deli system?
A That in conjunction with some other information I found in RAM, it did.
Q What was the other information you found in RAM?
A I found a process that was running in memory called "kameo." And when I extracted the memory segments from the kameo application and searched them, I found a large number of credit card numbers in those memory segments.
Q So what was your opinion as to what had occurred on the Schlotzky's Deli system?
A That the kameo malware had been installed, that it was harvesting credit card numbers, and then transmitting them to the server in Russia.
Q What did you do next?

A I wrote up a description of what I had found. I talked with the Secret Service agents and supervisors in Spokane and offered to assist them further with the investigation. And then I drove back to Seattle.
Q Okay. Once you drove back to Seattle, did you conduct further examination of the forensic image you had taken?
A Yes.
Q Did you examine the event logs from Schlotzky's Deli's computer?
A Yes.
Q What are event logs?
A Event logs are log files that are on the computer that note when certain events happen on a computer. They're diagnostic in nature, not something that your average user would need, but it's a diagnostic log.
Q What type of event logs do you typically review?
A The security event log, the application event log, and the software event log.
Q Are those always the same on every computer system?
A Yes.
Q What can you learn from the event log?
A You can learn who was logged into the system. You can learn what processes or applications are running on the system. You can see if remote access attempts were made into the system. There's many, many, many different things that can be

logged in the event logs.
Q So in preparing for trial, did you make copies of the files and forensic artifacts that you located during your exam?
A Yes, I did.
Q How did you make those copies?
A I extracted them from the forensic software and put them into a report.
Q I'm showing you what's been marked as Government's Exhibit 1.1. It's three pages.
Do you recognize this?
A Yes.
Q I'll go through all three pages.
How do you recognize this exhibit?
A These are screenshots from the forensic image that I took from Schlotzky's Deli in my examination.
Q Do these screenshots fairly and accurately represent the files and forensic artifacts you found on the Schlotzky's Deli system?
A Yes.
MR. BARBOSA: The government offers Exhibit 1.1.
THE COURT: Any objection?
MS. SCANLAN: No objection.
THE COURT: 1.1 is admitted.
(Exhibit 1.1 was admitted)
MR. BARBOSA: And may I just publish upon its

admission, Your Honor?

THE COURT: You may, Counsel.

BY MR. BARBOSA

Q Turning your attention to Page 1 of Exhibit 1.1, can you explain for the jurors what this shows us?

A Sure. So this shows six different files and one folder that were located on the Schlotzky's Deli back-of-house server.

Q Are these all the files that were on the computer?

A No.

Q Why did you select these particular files?

A Because these were the files associated with the hacking of the system.

Q And how did you determine that these were the files associated with the hacking?

A By my analysis of the RAM from the system, I had already determined that kameo was malicious software that was stealing credit card numbers. Based on the fact that it was created on the device on April 1, 2010, I then examined other activity that occurred in and around that time, and came up with this list of malicious files. This also matched with information we received from financial institutions related to when the compromised cards had recently been used at Schlotzky's.

Q Is there any particular reason why you included the last access dates on this exhibit?

A Just additional context.

Q Could you tell the jurors -- there's several files here, in addition to the kameo one.

What were the other files related to? Did you examine them?

A Yes.

Q Let's go through those. What is "shmak"?

A So shmak2 and kameo are both the pieces of malware that is designed to steal credit card numbers. So that's the actual malicious application that was on the machine.

Q Moving on to "sc.exe," what is that?

A That's "service create dot exe." What that does is, that's the persistence mechanism that was used to make sure that if the system was turned off and turned back on, that kameo would start up again. So a service is a way -- installing something as a service is a way to ensure that that will happen.

Q Why does this have a file created date of 1979?

A It's actually a Microsoft application. And so based on how that was moved over from the other system that was connected to this, it's not uncommon to see that July 31, 1979, date.

Q Moving to Page 2 of Exhibit 1.1 -- just a moment. I'll try and focus in on this a little bit better.

What are these snippets that we have here? Looks like hieroglyphics to most of the people in the courtroom.

A So this was some of the code that was visible in plain text at the end of the kameo executable and the shmak executable. So I can explain more in detail.
Q Yeah, let's go through that. So there's a couple of things highlighted here, and I assume these were not highlighted on the computer itself.
A No.
Q What is the purpose of highlighting these items?
A Just to make it easier for us to see, because it's pretty --
Q So drawing your attention to this "HTTP" line, what is that?
A So that is the location for where the stolen card numbers were going to be transmitted and the PHP script that would be called on the remote server.
Q All right. So let me slow you down a little bit.
How do you know that that is where the cards are being sent to?
A Based on the fact that I also reviewed RAM and saw an open connection to that IP address.
Q And you referred to a "PHP script."
A Yes.
Q What does that mean?
A PHP is a type of computer coding that allows interaction with a remote website.

Q And what did this tell you, based on your training and experience?
A That the malware was going to contact that IP address, and specifically the ftm.php script on that remote server.
Q And what would it do with the data that it had collected?
A Once it contacted the remote server, which was running PHP, it would then transmit the stolen credit card numbers to that script for the server to then process remotely.
Q So are these two different pieces of malware?
A No.
Q Why are there two different files here?
A Just named them differently.
Q And when had those been placed on the computer, based on your exam?
A April 1, 2010.
Q Okay. Were these pieces of malware operating the same, then?
A Yes.
Q Could you summarize for the jurors what your opinion is, based on your training and experience, as to how the kameo and shmak malware was functioning on Schlotzky's Deli system?
A The malware was installed on the system. It was monitoring those systems for -- specifically for credit card numbers. Once it had identified credit card numbers, it stored them for a period of time and then transmitted them to the

remote server as it collected them.
Q And that remote server, is this the IP address for it we see on Page 2 of Exhibit 1.1?
A Yes.
Q And where was that remote server?
A Russia.
Q Was the kameo and shmak malware well known at this time, in May of 2010?
A No.
Q Based on your training and experience, what did that tell you about the malware?
A That it was very unique, and that it was not what we would consider a commodity-based malware. It was assigned a very specific purpose and would only be installed on systems that were processing credit cards.
Q Would this have been detected by antivirus scanners?
A It was not at the time.
Q Why not?
A Because in order for antivirus to generate signatures for malware, they have to have first seen a piece of malware from that family. And because this malware was so new and so sparingly deployed, they hadn't seen it, and there were no signatures.
Q Turning to Page 3 of Exhibit 1.1, what is this?
A This is from the system event log.

Q And why did you select this event from the system event log?
A This is the system event log from April 1, 2010, showing that there was an RDP connection that had disconnected at 4:42 a.m., the same time frame as when the malware arrived on that system.
Q And what port would this RDP connection have been over?
A 3389.
Q Is that the same port that you had discussed earlier, when you were explaining how ports are used?
A Yes.
Q Based on your training and experience, did this lead to any conclusions about how the malware had been planted on the system?
A Yes.
Q What was that conclusion?
A That the system had been accessed remotely, that that remote user had been -- copy and pasted the malicious software onto that system, had installed it, and was then collecting it at the server in Russia.
Q So moving on in your investigation, at some point after you examined the Schlotzky's Deli system, did you learn that some of the compromised accounts had been used in Cleveland, Ohio?
A Yes.

Q When was that?
A In June of 2010.
Q How did you learn about this?
A The Secret Service agent in Spokane, who was working the Schlotzky's case, notified me.
Q What was the connection? Why were you contacted about this?
A The subject in Cleveland had been arrested with card numbers that had been originally used at Schlotzky's; so they tracked back to that common point of purchase. And that subject had a laptop with him, and there was potentially information on that laptop as to the source of those credit card numbers. So I was contacted to help determine who was selling the stolen card numbers from Schlotzky's Deli.
Q So did the agent in Cleveland provide you copies with any of the evidence he had obtained?
A Yes.
Q Did this include some of the stolen credit card numbers?
A Yes.
Q How were they provided to you?
A They were in a text file.
Q Was there anything you found of interest in relation to those text files?
A Yes.
Q What?

A The text files had a unique naming convention to them, or appeared to be unique to me, machine-generated.
Q What was unique about them?
A Specifically, the text files were order, dash, an order number, .txt. And there were two of them, and they were sequential. And in viewing that, it appeared that they were from a machine-generated process.
Q And why did that get your attention?
A It led me to believe that the cards had been purchased from an automated vending site.
Q At that point, did you seek any assistance from Secret Service agents in D.C.?
A Yes.
Q And did you begin coordinating with them?
A Yes.
Q Did they have any information helpful to you, without saying what the information was?
A They did.
Q Did you ask them for assistance in identifying these particular orders?
A Yes.
Q How did that, if at all, focus your investigation?
A They provided information on who they thought might be selling card numbers using that naming convention.
Q After that, did the agents in Cincinnati get you a full

forensic image of the computer?
A Yes, they did.
Q And were you able to examine it?
A Yes, I was.
Q What were you looking for?
A I was looking for the source of the stolen credit card data, so internet-related activity, chat-related activity.
Q What did you find?
A I found all of that.
Q Showing you what's been marked as Government's Exhibit 16.10, which is two pages, do you recognize that?
A Yes.
Q How do you recognize it?
A These are from a report that I created regarding my examination of the computer hard drive from Cleveland.
Q And are these forensic extracts from that hard drive?
A Yes.
Q Do they fairly and accurately represent the files and forensic artifacts you found on the image of the drive from Cleveland?
A Yes, they do.
MR. BARBOSA: The government offers Exhibit 16.10.
MS. SCANLAN: Your Honor, if I may have one moment?
THE COURT: You may.
Members of the jury, if you'd like to stand and stretch at

this time.

Please be seated.

MS. SCANLAN: Your Honor, the defense objects to the admission of this exhibit, based on the hearsay contained in the second page.

THE COURT: Counsel for the government?

MR. BARBOSA: Your Honor, these are offered as statements of a party opponent.

THE COURT: All right. The objection is overruled, based upon that proffer by the government. 16.10 is admitted.

And will it be subject to further connection, Counsel?

MR. BARBOSA: Yes.

THE COURT: Okay.

MR. BARBOSA: Is that conditionally admitted or admitted?

THE COURT: No. It's admitted.

(Exhibit 16.10 was admitted)

BY MR. BARBOSA

Q Displaying for you Exhibit 16.10, Page 1, what is the artifact we see on the top of Page 1 here?

A So that shows the file path to the text file that contained the credit card data. So we see the order, 3186.txt, and then the contents of that file, which starts with "438." So that's a 16-digit Visa card number with the separator, followed by the remainder of that track. And then the second

entry is for order 3187.txt, showing, again, another Visa credit card number.

Q Are these the automated order numbers you were referring to earlier?

A Yes, they are.

Q What is the second half of Page 1 of Exhibit 16.10?

A This is internet history that I extracted from that same laptop.

Q And why did you focus on this particular internet history?

A For a number of reasons. First, it shows the ICQ.com, which is the web address for the ICQ application for communication; Liberty Reserve, which was an online digital currency company; as well as bulba.cc, which was a credit card vending website.

Q Based on your review of this exhibit, this internet history, and your training and experience, what did this internet history tell you?

A That the Cleveland user had gone to bulba.cc and placed orders for credit card numbers. The order ID even matches the text file number.

Q Is that the highlighted portion, towards the bottom of the page?

A The very last; the 3186 matches the order, dash, 3186.txt.

Q Moving to Page 2 of Exhibit 16.10, what is this, and where did you find it?

A So this is from the ICQ chat logs that were on the system. And these are conversations between the user of the computer and the ICQ number 554716101.
Q And had you seen that ICQ number elsewhere?
A Yes.
Q Who had identified themselves as using that ICQ number?
A Track2.
Q Okay. So focusing on this first conversation, listed as March 29, 2010, is that your annotation, the dates?
A That's correct.
Q I believe one of these is --
A The very -- the second to the last, the March 5, 2010, is actually May 5, 2010, as you can see by the dates farther over to the left. I just typed "March" instead of "May" on accident.
Q Okay. So who is the speaker for the first line?
A The speaker for the first line is the gentleman in Cleveland.
Q And then the second line would be?
A Track2.
Q Can you go through this conversation for the jury?
A Sure. So the Cleveland purchaser statement, "Hey, bro, what is the new site?" And then track2 responded, "www.track2.name."
Q Go ahead. What was the next conversation about?

A On April 7, 2010, the Cleveland buyer, "Bro, what I have to do to gain access to your site?" And then track2 responded, "Registration close."

Q What did that mean, "Registration close"?

A They're no longer accepting new users to that site.

Q Did you ever try and visit the track2 site to see if it was, in fact, closed to registration?

A Yes.

Q What did you find?

A It was closed.

Q The next conversation, what was the nature of that?

A April 26, 2010, the Cleveland user, "Got any good dumps?" Track2 responded, "Look in site." The Cleveland user responded, "Been trying to become member, but was told registration was closed." Track2 responded, "For register need to pay 1,000 deposit." And Cleveland user, "Come on, bro, trying to get my money up, bro. Have a little WM," which stands for WebMoney, "but nothing." Track2 then responded, "It's your problem."

Q At some point, did track2 direct this person to another site?

A Yes.

Q Is that the next conversation?

A Yes.

Q Can you go through that?

A May 5, 2010, the Cleveland user states, "Need dumps," and then, "Need dumps, sis." And then track2 responds, "www.bulbacc. You can make account there. It's our official reseller."

Q And then the final message from track2, what was that?

A That was from track2, on June 6, 2010, "Tomorrow biggest update of the year. More than 100,000 dumps."

Q And to clarify, when we went over the fact that the site "track2" was closed for registration, does that mean it wasn't operating anymore?

A No. It was operating. It just wasn't accepting new users.

Q Approximately when was it that you examined the Cleveland drive and found this connection between Schlotzky's and these potential vending sites?

A It would have been July 2010.

Q So after you discovered that connection, did you start researching these sites that we just saw in the chat?

A Yes, I did.

Q What type of information did you look for in relation to the bulba and track2 sites?

A In addition to visiting the sites and seeing what the content was, I also looked at the domain registration information, as well as the location for where the sites were being hosted, so what IP address they were located at.

Q Let's talk, first, about your visits to the sites and what you found there.

Did you take screenshots, pictures, of the websites, as you visited them?

A Yes, I did.

Q Can you explain for the jury what a screenshot is?

A So using an application on my computer, I'm able to take a picture of what I see on the screen at that given time.

MR. BARBOSA: Can the courtroom deputy provide the witness with the binder with Exhibits 2.1 to 2.3? I think it's probably Volume 1.

BY MR. BARBOSA

Q If you could look in the binders so I don't have to thumb through each one of these, I'd like you to look at Exhibits 2.1 through 2.3. So we're probably talking somewhere in the neighborhood of 20 pages.

Just let me know once you've had a chance to look through those.

A Okay.

Q Do you recognize all those?

A Yes.

Q How do you recognize those exhibits?

A These are screenshots that I took from bulba.cc and track2.name.

Q Do they fairly and accurately show how the websites

appeared when you visited them as part of your investigation?
A Yes.
MR. BARBOSA: Government offers Exhibits 2.1 through 2.3.
MS. SCANLAN: Your Honor, the defense objects to the admission of 2.3 on the grounds that it's hearsay, and the government has not laid a foundation for any exception.
THE COURT: One second, Counsel.
Counsel, on 2.3?
MR. BARBOSA: Same reason for admission, Your Honor. We believe these are statements of a party opponent. They are the bulba website. We are also offering them as substantive evidence. They are effectively the crime scene. This is the website that exists. This is what he saw.
THE COURT: The objection is overruled. 2.1 through 2.3 will be admitted.
(Exhibits 2.1 through 2.3 were admitted)
BY MR. BARBOSA
Q Let's start with Exhibit 2.1. And this is just one page.
What is this that you have taken a screenshot of here?
A This is the primary page that any user would have seen if they had typed in "bulba.cc" and been directed there. So this is where you can either log in, if you already have a username and password, or where you could register for a new account, if you had not done so yet.

Q So is this the first landing page, when you arrive?
A Yes.
Q And the address shows "secure.bulba.cc." Is that what you had typed in, or did you --
A No. You would have been redirected to that.
Q And there's a second tab open in your internet browser. What is that?
A That was the other site that I had open at that time, which was track2.name.
Q And the date appears in the lower right-hand corner. Is this when you were doing this initial investigation?
A Yes.
Q Taking you to Exhibit 2.2, is that simply the other tab you had open in your browser, at that point?
A That's correct.
Q So what do we see here?
A This is the splash page, or landing page, for track2.name.
Q Are they similar?
A They were almost identical.
Q Were you able to open accounts on either of these sites?
A I was able to open an account on bulba.cc.
Q Moving to Exhibit 2.3, let me bring this up on a single screen.
MR. BROWNE: Sorry, Mr. Barbosa. Which exhibit did you say?

MR. BARBOSA: 2.3.

BY MR. BARBOSA

Q And this is a total of 15 pages.

Starting with the first page, what did you see after you were able to establish an account on bulba?

A So after establishing an account and logging in, you would then be taken to the main page for bulba.cc, where there would typically be announcements posted for people to read.

Q And this announcement on Page 1 of Exhibit 2.3, is that typical of the announcements you saw when you visited the site?

A Yes.

Q Could you go over this for the jurors?

A Sure. Do you want me to explain it as I'm going through it?

Q Please, yeah.

A "Update 17,000 fresh dumps. Totally made, valid. Very high, 95 percent."

Q Based on your training and experience and your experience with carding investigations, what does this comment, "Totally made," mean?

A It means that they're very good. So there's 17,000 unique credit card tracks that are very good, with a 95 percent chance that if you use them, they will work.

Q Okay. And further down, we have "Base New 65" -- sorry. I'm not going to do that again. I tried to focus in on that,

and it did not work.

What is "Base New 65"?

A So that's the name of the database that contains these 17,000 card numbers.

Q And the comment, "Warning, today checker not work," what is a "checker" in the carding industry?

A So on some carding sites, there is what's called a checker, which gives the purchaser the opportunity to check if the card is still valid. So you can pay sometimes a few pennies or a quarter, and after you purchase a card, they'll run it through another criminal service that verifies if the card is going to be accepted through the card brands. If it is accepted, you keep the card. If it's not accepted, most card vending sites will replace it for you for free.

Q Moving to Page 2 of Exhibit 2.3, there are a number of tabs on the website.

Did you explore each of those, and can you tell the jurors what -- where these would take you?

A Sure. So moving from left to right, "dumps," if you were to click on "dumps," you would be provided with a screen where you could search for specific credit cards that you wanted. So you could search by BIN number. You could search by bank, and as well as a number of other fields. "Orders" were the orders that you had made. "Profile," you could add profile information. "Billing" had to relate to funding your actual

account. The "checker" service was what I spoke about earlier, your ability to check those card numbers. You could contact support. There was a support page where you could write messages to the administrators of the account. And then you could sign out, log out. The username, that was my undercover username at the time. And then a balance of zero, I didn't have any money in my account at that time, and I had zero checks available.

Q The balance of the pages in Exhibit 2.3, are these additional news updates that you found when you visited the site?

A They are.

Q What did the bulba website accept for payment?

A Online currencies and Western Union, typically.

Q What types of online currencies?

A Liberty Reserve, WebMoney, were the two primary.

Q Were you familiar with these payment methods?

A Yes.

Q What is Liberty Reserve?

A Liberty Reserve, at the time, was an online currency that existed. It was tied to the U.S. dollar, although not sanctioned by any nation or state. It was -- but it was basically a banking system for people that didn't want to use the traditional means. It was very commonly used among computer hackers.

Q During the course of your investigation, did you make any undercover purchases through this site?
A Yes.
Q How did you go about making the purchases?
A The first thing I did was contact the administrators on the page to ask them where I could send a Western Union transfer. I was provided with Western Union transfer information to Vietnam. I then went to a Western Union and sent money to that name. And a few hours later, the money was posted to my online account at the site.
Q In your training and experience, was this method of using Western Union to provide payment -- was that common in the carding industry?
A Yes.
Q Was that a lead that you were able to follow up on?
A Yes.
Q What did that name lead to? The name that you were provided, was that helpful in your investigation?
A The name that I transferred money to was not helpful, no.
Q Why not?
A It was what's called a "drop," or a "money mule," so somebody whose job it is to collect Western Unions and then forward them on to somebody else.
Q Once you purchased cards, were you able to confirm whether they were real credit cards?

A Yes.
Q How did you go about doing that?
A I specifically purchased cards from the Boeing Employees Credit Union. And then after purchasing those cards, I provided them to the Boeing Employees Credit Union to validate that they were legitimate cards.
Q Did you receive records back on those cards?
A Yes.
Q So after you conducted your initial review of the websites, did you put together a plan for investigating these sites?
A Yes.
Q When was that, approximately?
A That would have been in late summer of 2010.
Q And what was your plan? What were you going to look for?
A Ultimately, to track down any information we could regarding the infrastructure associated with the track2 and bulba websites, as well as any other information we could find from carding forums regarding the nicknames "track2" and "bulba.cc."
Q And what did you learn about the infrastructure? What information was available to you publicly about the -- these websites?
A So we could determine who had registered the websites, the name they had provided, the e-mail address that they provided,

and a telephone number that they had provided. We could determine who they registered the domains through. We could determine the IP address for where the sites were currently being hosted. We could -- through ICQ, we could determine information related to the registered party for the ICQ numbers.

Q What was the goal as you identified IP addresses for the domains or e-mail addresses used to register them?

A Try and determine who was running the infrastructure for the sites.

Q And how would you do that? How would you get ahold of this information?

A Through core process to various e-mail providers, internet service providers, domain registration companies, any company that had records related to what we were -- the information we were finding.

Q Were you continuing to work with agents in Washington, D.C.?

A Yes.

Q Who did you work with primarily from D.C.?

A Special Agent Keith Wojcieszek.

Q And how did you coordinate your investigation with Keith Wojcieszek? Did you split up your duties?

A We did split up the duties, yes.

Q How did you divide the responsibilities?

A It depended on what things were occurring at that time. Keith primarily focused on e-mail search warrants, and later on on serving warrants for data that was located on the East Coast.

Q Did he also have access to historical information?

A He did.

Q Did you and Agent Wojcieszek conduct any research to attempt to identify -- well, you just said that you looked into the domain registrations. Let me ask you about that.

How did you look into the domain registrations for these websites?

A So we conducted what's called a "Whois Lookup."

Q What is a "Whois Lookup?"

A So a Whois Lookup is basically querying the "who is," or the phone book type information, for domain registration. So it's publicly available information to determine who to contact regarding a domain or an IP address.

Q And were you able to go -- to determine what the IP addresses for these websites were?

A Yes.

Q What did you learn about the IP addresses for both bulbacc and track2.name at that time?

A That they were hosted together. And they were the only two websites that were hosted, and they were not hosted in the U.S.

Q Do you know where they were hosted?
A I believe they were in the Ukraine.
Q Did you attempt to get ahold of those websites, or copies of the servers?
A Yes.
Q Was that successful?
A No.
Q So we've gone over domain names and what they are, but I'm going to have you take a look at Government's Exhibit 4.5. We talked about researching domain registration records.
Can you look at that, in the notebook in front of you, Exhibit 4.5?
A Do you want me to review the whole thing?
Q Does it look -- you've reviewed it before; is that right?
A Yes.
Q Is that the same one?
A Yes.
Q Okay. And what is it, specifically?
A This is the domain report from DomainTools on the domain name track2.name.
Q And is that approximately over 90 pages; is that right?
A That's correct.
Q What type of information, without the specifics, is contained in these reports?
A The name of the registrant, their e-mail address, physical

address that they had provided, phone number that they had provided.

Q And are these reports publicly available?

A Yes.

Q And are they generally relied upon by people in the computer networking industry?

A Yes.

MR. BARBOSA: The government offers Exhibit 4.5.

THE COURT: Any objection?

MS. SCANLAN: Your Honor, the defense renews the objection from the pretrial conference.

THE COURT: The objection is noted. It's overruled. It's admitted.

(Exhibit 4.5 was admitted)

MR. BARBOSA: Thank you, Your Honor.

BY MR. BARBOSA

Q All right. I'm going to turn your attention to quite a few pages into this, Page 86, Exhibit 4.5.

What was the date this registration check was completed?

A March 3, 2010.

Q Was that approximately around the time you were conducting your investigation?

A Yes.

Q And do the records in the domain registration for track2.name, in Exhibit 4.5, continue to update the domain

registration records throughout your investigation?
A Yes.
Q So is this information consistent with what you saw throughout your investigation?
A Yes.
Q When was the website track2.name registered?
A It was registered on March 3, 2010.
Q Is that highlighted about five lines down?
A Yes.
Q And who was the name listed as the registered owner of the site?
A Alexey Davydov.
Q Does it tell you what e-mail address was used to register it?
A Yes.
Q Where is that?
A It's right there, rubensamvelich@yahoo.com.
Q What parts of this information were you interested in?
A The e-mail address.
Q Why the e-mail address?
A That's the manner in which the registrant will be contacted in the event that there are abuse complaints or other issues related to the domain.
Q Does that -- is that used for billing, in your experience?
A Yes.

Q Let's take a look at Exhibit 4.4. Again, this is 50 pages.

If you could look at it and just confirm whether or not that's another domain registration record that you recognize?

A Yes, it is.

MR. BARBOSA: Government offers Exhibit 4.4 under the same exception.

MS. SCANLAN: Your Honor, the defense has the same objection.

THE COURT: Same ruling. 4.4 is admitted.

(Exhibit 4.4 was admitted)

BY MR. BARBOSA

Q What is this for?

A This is the domain report for the domain bulba.cc.

Q And I should have highlighted this earlier. There was a similar page on the beginning of 4.5.

Is this a screenshot that's included with the domain registration record?

A DomainTools takes that screenshot as part of their service.

Q Turning to Page 48 of Exhibit 4.4, when was the bulba site registered?

A April 26, 2010.

Q And what was the registration name and e-mail address provided?

A Valentin Chinakov. And the e-mail is bulbacc@yahoo.com.
Q So during your investigation, did you pursue any process to look at these e-mail accounts?
A Yes.
Q Did you also find sites with domain names similar to the track2.name site?
A Yes.
Q Approximately how many?
A I believe three or four others.
Q And do you recall any of the names?
A Track2.tv, track2vip.tv. Just off the top of my head, that's what I remember.
Q And did you try and visit those sites to confirm if there was any relation between them?
A Yes.
Q What did you find?
A They were not up when I visited.
Q So you didn't find them?
A Yeah.
Q Did you look into registration records for them?
A Yes.
Q Why did you look for registration records for those sites?
A For the same reason I was looking at track2 and bulba.cc, to try and determine and build out the infrastructure in the investigation.

Q Did you find any similarities?
A Yes.
Q What were those similarities?
A The registration addresses.
Q Okay. Can you take a look in the binders in front of you -- and I won't bring these up on the overhead -- 4.8 to 4.10?
A I don't have that binder. I only go to 4.5.
THE COURT: Members of the jury, if you want to stand and stretch real quick?
Please be seated.
Counsel?
MR. BARBOSA: Thank you, Your Honor.
BY MR. BARBOSA
Q What are those exhibits, 4.8 through 4.10?
A They are similar reports for track2.tv, track2vip.tv, and track2.cc.
MR. BARBOSA: The government offers Exhibits 4.8 through 4.10 under the same exception.
MS. SCANLAN: Your Honor, the defense renews their objection to all three of those exhibits.
THE COURT: So noted. 4.8 through 4.10 are admitted.
(Exhibits 4.8 through 4.10 were admitted)
BY MR. BARBOSA
Q I'm seeing these are pretty long. Would it be more

convenient to go over --

MR. BARBOSA: I think 4.9 also. Is that also admitted?

THE COURT: You said 4.8 through 4.10. So the "through" meant they're all included.

MR. BARBOSA: Thank you.

BY MR. BARBOSA

Q Would it be more convenient to review the information from those reports in a summary form?

A Yes.

Q Okay. And have you seen a summary of all the registration information for those sites?

A Yes, I have.

Q I'm going to show you, on the overhead, what's been marked as 4.12.

Do you recognize that?

A Yes.

Q What is it?

A It's a summary of the registration date, registration name, registration e-mail address, phone number, and street address for the five domain names.

Q And have you checked this against the registration records admitted as 4.4, 4.5, and 4.8 through 4.10?

A Yes, I have.

Q Does it accurately represent the information in those

records?
A Yes, it does.
MR. BARBOSA: Government offers Exhibit 4.12.
MS. SCANLAN: Your Honor, the defense renews our objection. This is not a proper summary exhibit.
THE COURT: Overruled. 4.12 is admitted.
(Exhibit 4.12 was admitted)
BY MR. BARBOSA
Q All right. Could you highlight for the jury some of the similarities you noticed?
A Sure. So three of the domain names have the same registration e-mail address. That would be track2.name, track2.tv, and track2vip.tv. They were all registered with rubensamvelich@yahoo.com. There are similar addresses for track2.tv and track2vip.tv. The phone number for track2.name and track -- and bulbacc are very similar, with the exception of the very last digit. One has an "8," and the other has a "1."
Q You mentioned, also, looking at the IP addresses for these sites.
What was the purpose of trying to locate the IP address?
A To -- the ultimate goal would have -- if possible, to seize the servers.
Q And how did you go about figuring out what the IP address was?

A Running a tool on my laptop, as well as searching through domain records.

Q I'm showing you what's been marked as Government's Exhibit 4.11.

Do you recognize that?

A Yes.

Q What is it?

A This is a reverse IP address lookup. So basically, it tells you what websites are hosted at a specific IP address.

Q And is that information also publicly available?

A Yes.

Q And that's a two-page exhibit.

Does that have additional information on the second page that's publicly available?

A Yes.

Q What type of information, without specifics, does this provide you?

A It shows that there are two sites that are hosted there, bulba.cc and track2.name, as well as an anti-DDoS provider.

MR. BARBOSA: The government offers Exhibit 4.11.

THE COURT: Counsel?

MS. SCANLAN: No objection.

THE COURT: 4.11 is admitted.

(Exhibit 4.11 was admitted)

////

BY MR. BARBOSA

Q So looking at Page 1 of 4.11, what is this showing you?

A That those two sites are hosted at IP address 213.186.112.132.

Q And the second page of this exhibit, what does it tell you about that IP address and those sites?

A That it's part of the Ukrtelecom, in Kiev, Ukraine. And that in addition to that, there's records related to antiddos.biz.

Q What did you learn about antiddos.biz?

A That antiddos.biz provides distributed denial of service protection for websites.

Q Why would somebody use distributed denial of service protection for a website like this?

A Because their website was being attacked by a DDoS.

Q How does -- based on your training and experience, how does a DDoS protection service operate? What does it provide for the website?

A They provide a number of different services, depending on the type of DDoS. There are many different DDoS attacks that can be perpetrated against a website. So the anti-DDoS services mitigates those attacks. They identify what kind of attack is coming in, and then they utilize countermeasures to get rid of the bad traffic and allow the legitimate users to access the website.

Q Does the use of an anti-DDoS service have any impact on the true location of the IP, or your analysis of the true location of the IP address for the website?
A Yes, it does.
Q How?
A Because the -- all traffic routed to the website is proxied, or sent through the DDoS provider. So the IP address that you get is the IP address for the DDoS provider, not the true location for the website.
Q So what does that mean in terms of your ability to identify the true location of the website?
A That the only way to do that would be to contact the anti-DDoS provider to get that information.
Q And were you able to do that in this case?
A No.
Q Why not?
A Because it's an anti-DDoS provider that's located in the Ukraine.
Q So after you and Agent Wojcieszek did this initial research, looked at the IP address and found the registration records, what did you do next?
A We obtained core process for contents of the e-mail addresses that we had identified that were located within the U.S.
Q And which e-mail addresses were those?

A Rubensamvelich@yahoo.com and bulbacc@yahoo.com.
Q And to refresh, which of those related to which website?
A So rubensamvelich@yahoo.com was used for track2.name. And bulbacc@yahoo.com was used for bulba.cc.
Q When did you obtain these search warrants?
A They were obtained in the fall of 2010.
Q Which of you, Agent Wojcieszek or yourself, obtained the search warrants?
A The original search warrants were obtained by Agent Wojcieszek.
Q When you get a search warrant for an e-mail account, do you actually go to Yahoo! and take the e-mails off their servers?
A No.
Q How do you go about executing a search warrant for an internet-based e-mail account like that?
A The internet e-mail providers typically have a contact, a legal process contact, who will accept search warrants, most commonly by fax. So you send a fax copy of the search warrant to the provider, and then they return the results -- or the contents of the mailbox and anything else specified in the search warrant to you via CD or DVD, in the mail.
Q How long does it usually take to receive the contents and other information back?
A It really depends on the provider, sometimes a month,

sometimes a couple months.
Q What do you do once you get the information? And did you say it comes on a disk?
A Yes.
Q What do you do once you get the disk back from Yahoo!?
A You copy the contents of the disk so you can review it. The disk gets placed into evidence, and then you review the data.
Q What did you look for in these accounts?
A Information related to the infrastructure being used, information related to the people involved in the case, basically any information I could find regarding the theft and sale of credit card numbers or any infrastructure necessary to support them.
Q Did you look for indications of who was using the accounts?
A Yes.
Q In general, can you describe what you found in the contents of the e-mail account rubensamvelich?
A So in the account rubensamvelich, I found information related to the lease of servers located both in the U.S. and abroad. I found registration records for websites associated with it. I found information related to other accounts, such as PayPal, and others, that were included in the account.
Q So in addition to the content of the account, you

mentioned that Yahoo! sometimes provides other information.

What type of other information do they provide?

A The account registration information, as well as IP address information for the most recently -- the most recent IPs that have been used to access the account.

Q Can you take a look at Exhibit 6.1 and tell me if you recognize that?

A I do.

Q This is two pages. How do you recognize that?

A That's the printout from the Yahoo! account management tool that shows the registration information for the e-mail account rubensamvelich@yahoo.com.

MR. BARBOSA: The government offers Exhibit 6.1, Your Honor.

THE COURT: Any objection?

MS. SCANLAN: Yes, Your Honor. There's been no foundation for this exhibit, at this point, as a business record, with this witness. There's been no foundation laid through this witness for this exhibit.

THE COURT: Counsel?

MR. BARBOSA: The government is still offering this under a 902 certification that the Court ruled on earlier.

THE COURT: All right. The objection is overruled based on the Court's prior ruling. That's 6.1.

(Exhibit 6.1 was admitted)

MR. BARBOSA: Thank you.

BY MR. BARBOSA

Q What is this that we're looking at in Exhibit 6.1?

A So this is the registration information for the account. So we have the login name of rubensamvelich; that it's for the Yahoo! mail property, or that service; the e-mail address, rubensamvelich@yahoo.com. There's a registration IP address for when the account was created, the date that the account was created, the full name for the account holder, the country and zip code where the account holder says they're from, as well as the birthday and gender that were provided by the account holder.

Q Are you familiar with how this information is supplied to Yahoo!?

A Yes.

Q Who supplies the information in this record?

A So it depends on which piece of information. Some of it is automatically generated, and some is provided by the user. For example, the user uses the login and the Yahoo! mail name. The registration IP and account created date are automatic processes by Yahoo!, as part of creating the account. The account holder name, country, zip, birthday, and gender are all provided by the user.

Q Do you rely upon the name on an internet e-mail account to identify the user?

A Not solely, no.
Q Why not?
A Because you can put anything in there.
Q Moving to Exhibit 6.2, which is several pages long, six pages, approximately, do you recognize that?
A Yes.
Q How do you recognize that?
A These are the IP addresses that were provided by Yahoo! for the most recent account logins to the rubensamvelich e-mail account.
Q And what does that mean, the IP addresses for the account?
A So every time the user logged into the account, Yahoo! recorded the IP address from where the user logged in from.
Q And how is that information supplied? Is that supplied by the user?
A No. It's the information the Yahoo! servers captured when the login session occurs. So it's an automatic process.
MR. BARBOSA: Government offers Exhibit 6.2.
THE COURT: Defense?
MS. SCANLAN: Your Honor, I just had a question regarding the exhibit.
There was some highlighting on the exhibit, just now, that's not currently present. I'm wondering if that is considered a portion of the exhibit, or not?
THE COURT: Are those counsel's highlights?

MR. BARBOSA: This is my highlighting. I can take it off for now and highlight it later.

MS. SCANLAN: Maybe I'm not being clear. I guess my inquiry was whether the idea is that it's going to be admitted into evidence with the highlights, or not.

THE COURT: What I have before me, Counsel, which is, I believe, a duplicate of what's before the witness, there are no highlights. So that's the exhibit that will be admitted for purpose of the jury's consideration. Counsel may highlight that for purpose of examination, but it's not admitted in that format.

So any continuing objection?

MS. SCANLAN: No, Your Honor.

THE COURT: All right. With that, 6.2 is admitted.

(Exhibit 6.2 was admitted)

MR. BARBOSA: All right.

THE COURT: Counsel, it's 2:45. Would it be a good time to take our afternoon break?

MR. BARBOSA: Absolutely.

THE COURT: Members of the jury, we'll take our afternoon break.

(Jury exits the courtroom)

THE COURT: Counsel for the government, anything to take up?

MR. BARBOSA: One matter. I'd like to ask if we

could use Exhibit 17.7, which is a demonstrative exhibit. I'm just about to go further into discussions of the infrastructure, and that exhibit would help the witness in doing his testimony. It's a large board. I can actually show it for counsel.

THE COURT: Has counsel seen it?

MS. SCANLAN: No.

MR. BARBOSA: Yes, they have.

MR. WILKINSON: It was an exhibit used in opening statement.

THE COURT: Do you have any objection to --

MS. SCANLAN: I haven't seen the board, Your Honor.

THE COURT: Okay.

MR. BARBOSA: It's the same thing, just bigger.

MS. SCANLAN: As a demonstrative exhibit?

MR. BARBOSA: As a demonstrative.

MS. SCANLAN: I have no objection to that.

THE COURT: You have to make a formal offering in front of the jury, Counsel.

MR. BARBOSA: Okay.

THE COURT: Anything else to take up, by the government?

MR. BARBOSA: Just can I leave it up here so I don't have to walk back and forth?

THE COURT: Sure.

Anything else to take up, by the defense?

MS. SCANLAN: No, Your Honor.

THE COURT: Counsel for the government, I want to let you know that I'm going to interrupt about every 25 minutes just for a break for the jury, I think for obvious reasons.

MR. BARBOSA: I need the break too. I appreciate it.

THE COURT: We'll be in recess.

(Recess)

(Jury enters the courtroom)

THE COURT: Counsel, you may continue your direct examination of the witness.

MR. BARBOSA: Thank you, Your Honor.

BY MR. BARBOSA

Q So we were looking at Exhibit 6.2 when we stopped for the afternoon break. And I've highlighted Page 1, or focused in on the bottom of Page 1, these IP addresses.

What's the source of the information? Where does this come from?

A This came from Yahoo! business records.

Q What are these records? What is it showing you?

A Showing the IP addresses that were most recently used to access the rubensamvelich e-mail account.

Q And do you use these in conducting your investigations?

A Yes.

Q How do you use them?

A Researching these IP addresses can lead to information related to where the computer that was accessing the e-mail account is physically located.
Q So these IP addresses toward the bottom of Page 1 of Exhibit 6.2, are there any shown here that you were able to identify at some point in your investigation?
A Yes.
Q Which one?
A The three that start with "66."
Q And what's that full address?
A 66.36.240.69, 66.235.184.36, and 66.36.228.124.
Q Were you able to identify those servers and where they were located?
A Yes.
Q Do those IP addresses, that have been used to log in to the rubensamvelich account, did they come up elsewhere in your investigation?
A Yes.
Q Would it help you to explain to the jury how these IP addresses and the e-mail accounts, and the other infrastructure that you've discussed, relate to each other, to use a diagram?
A Yes.
MR. BARBOSA: The government offers Exhibit 17.7 as a demonstrative exhibit, the board that's on display now.
MS. SCANLAN: No objection.

THE COURT: 17.7 is admitted for demonstrative purposes only, and you may publish.

MR. BARBOSA: May the witness approach the exhibit?

THE COURT: You may.

BY MR. BARBOSA

Q And I'll just advise you to be a little careful. The stand there is slightly touchy.

A Okay.

THE COURT: Let's make sure, first of all, that all members of the jury are in a position to see this. Otherwise, we can -- the jurors have indicated no, Counsel.

If you'd like, you can have it moved a little bit closer.

MR. BARBOSA: Certainly. I can help you.

THE COURT: Can defense counsel see it?

MR. BROWNE: Yes.

MS. SCANLAN: Yes, Your Honor.

MR. BROWNE: We have a copy.

THE COURT: Now, are the jurors in a position to see the exhibit?

JUROR: Not the very, very bottom.

MR. BARBOSA: We may need to highlight it. I can bring it up on the overhead too.

THE COURT: Let's put it in two places, Counsel.

MR. BARBOSA: Sure.

////

BY MR. BARBOSA

Q All right. So we've been going over the rubensamvelich account, and you talked about some domain records earlier.

Can you explain for the jurors how the rubensamvelich account ties in to your investigation, using the Exhibit 17.7?

A So within the rubensamvelich e-mail account, there were records related to the leasing of servers, specifically a number of servers at a HopOne data center, located in McLean, Virginia. One of those servers, the primary one in the case, had IP address 66.36.240.69.

Q Is that the one you saw, just moments ago, in Exhibit 6.2, the login records?

A Yes.

Q So it was also logging into the rubensamvelich account?

A Right. So this server was logging into rubensamvelich, and it was also being leased from the e-mail account rubensamvelich.

Q Okay. Going back up to the rubensamvelich account, what was it related to?

A So rubensamvelich was related to the track2.name domain registration records, so the site that was vending the stolen card data.

Q And, now, in the lower left-hand corner, what is the server down there?

A So there was a server located at IP address

188.120.225.66. This server was located in Russia. And that was the server that was used to download the malicious software onto the victim point-of-sale server. So once the hacker had gained access to the point-of-sale server, he would direct the web browser to this server to download the malware, whether it be -- there were three versions of the malware -- primary versions of the malware. Schlotzky's just had one of the three.

Q And was that server used for any other purpose besides just downloading the malware?

A It also received stolen card numbers.

Q Okay. So moving back to -- let's go back to the right side of this Exhibit 17.7, the HopOne server that you identified based on the login IPs.

Based on your training and experience, did you draw any conclusions as to how that server fit into your investigation?

A So the HopOne server filled multiple roles in the investigation. It was used as a collection point for stolen credit card numbers. So one of the pieces of malware would direct the stolen card numbers to this IP address. This server was also used to scan large ranges of IP addresses for Port 3389, to see if there were servers that would be vulnerable to an attack. And then the server was also used almost as a personal computer, to browse the web and to view a number of various websites.

Q Okay. So now let's move back to rubensamvelich. You were talking about your review of that account.

Again, why was the registration e-mail address for the track2.name site -- why was that something you were focused on in the registration records?

A It's the most valid piece of information that you're going to get off a registration.

Q Why is that?

A Typically, you would have to create an account with a company that will register IP addresses. They'll send you a confirmation e-mail to confirm that you have a valid e-mail address. And so -- and people will provide valid e-mail addresses so they can address any kind of abuse complaints or other issues related to the site, billing, everything.

Q Is that why you focused your investigative efforts on that account?

A Yes.

Q Okay. So if you could go ahead and take your seat again.

When we reviewed the subscriber records for the rubensamvelich account that were in Exhibit 6.1, you saw the name "Mr. Romper Stomper."

A Yes.

Q Did you find any other names that the account holder used to send and/or receive e-mails in that account?

A Yes.

Q What were some of those names?
A Roman Seleznev, Roman Ivanov. There were a couple others in there, as well, but those are the two off the top of my head.
Q What about the name of the e-mail account?
A Oh, yeah, rubensamvelich, of course. Sorry.
Q Were there any nics used?
MR. BARBOSA: And let me ask, can Juror Number 15 see the witness? If we need to move that board, I can do it.
JUROR: Yes.
BY MR. BARBOSA
Q All right. I'm going to show you what's been marked as Government's Exhibit 6.3 and 6.3A, the translation.
Do you recognize those?
A Yes.
Q How do you recognize those?
A These are e-mails that were sent from PayPal to the rubensamvelich@yahoo account.
Q And is the first page of 6.3 -- is that an exhibit in Russian?
A That's correct.
Q So this has also been translated?
A Yes.
MR. BARBOSA: The government offers Exhibit -- actually, let me ask a few more questions.

BY MR. BARBOSA

Q So without describing the contents of these e-mails -- you mentioned it was a PayPal e-mail -- can you describe the nature of that e-mail from PayPal?

A It was a welcome e-mail to an account holder.

Q When someone opens a PayPal account, who supplies the PayPal account information?

A The person that's opening the account.

Q So what is the source of the information in a welcome e-mail?

A That's automatically generated from PayPal, based on the information that had been submitted by the user.

Q And based on the information submitted by the user who opened the account?

A That's correct.

MR. BARBOSA: Government offers Exhibits 6.3 and 6.3A.

MS. SCANLAN: No objection.

THE COURT: 6.3 and 6.3A are admitted.

(Exhibits 6.3 and 6.3A were admitted)

BY MR. BARBOSA

Q So is the exhibit on the right-hand side, 6.3A, is that just simply a translation of the exhibit you found?

A Yes, it is.

Q And where was this, again?

A This was in the rubensamvelich@yahoo e-mail account.
Q And who was it addressed to?
A "Welcome, Roman Seleznev."
Q Did it provide any other identifying information for the person it was addressed to?
A Yes.
Q What was that?
A It provided the e-mail address, as well as a physical address.
Q I'm going to show you what's been marked as Government's Exhibit 12.6 and admitted as 12.6B, the translation of Mr. Seleznev's internal passport.
Is that the same address?
A Yes, it is.
Q Turning your attention to the second page of Exhibit 6.3, what did this e-mail address?
A This is from PayPal to Roman Seleznev, the subject being, "You have added a credit card." And it says, "Hello, Roman Seleznev. On September 22, 2009, the credit card ending in 8729 was added to your PayPal account. Thanks, PayPal."
Q What is the significance of adding a credit card account to a PayPal account?
A There's two primary reasons you would do that. One would be to help verify your account, and then the second would be so that you could use that as a payment source for PayPal

transactions.
Q Were you able to obtain any records from PayPal related to this account?
A Yes.
Q Showing you Government's Exhibit 15.5, do you recognize that?
A Yes.
Q How do you recognize Exhibit 15.5?
A It's the account information that was provided by PayPal.
Q And that's a four-page exhibit.
Does it contain information related to the PayPal purchases and other details?
A Yes, it does.
MR. BARBOSA: Government offers Exhibit 15.5 under a 902 certification.
MS. SCANLAN: No objection.
THE COURT: 15.5 is admitted.
(Exhibit 15.5 was admitted)
BY MR. BARBOSA
Q Turning your attention to the upper left-hand corner, what user information did PayPal have on record for this account?
A First name of Roman, middle name "V," last name Seleznev, date of birth, July 23, 1984, e-mail rubensamvelich@yahoo.com.
Q And did the account holder provide any other identifying information that's down in the lower --

A There's a telephone number.
Q What about the address?
A And there's an address.
Q What I've highlighted now, towards the bottom of the page?
A Yes.
Q Was that the same address you'd seen in the passport translation?
A Yes.
Q Turning to Page 2, did you see the credit card number that had been referenced in the e-mail receipt you found in the rubensamvelich account?
A Yes.
Q Is that the "8729" number?
A That's correct.
Q Did finding this PayPal record have any significance to your investigation?
A Yes.
Q Why?
A PayPal records are -- carry more validity than the other records we'd seen up to this point in the case.
Q Why is that?
A PayPal is a regulated entity, so it falls under a number of financial regulations that e-mail providers and others don't. So they have customer rules, verification steps, that are required and are checked for validity.

Q What about this comment on the right-hand column, "Personal Russian, unverified"?

A So as part of the PayPal process, you can have a verified account. What that means is that they will submit a small charge to an account that you have, and then you can -- so they may make a charge, like, $2.17. They don't tell you the exact amount for the charge. And then you go back to the site, and you say: Hey, I can access this account online. I know it was $2.17. And you can verify that you do have control and access to that card.

Q Does that decrease your reliance on this exhibit at all?

A No.

Q I'm going to show you -- well, actually -- sorry. Moving back to Exhibit 15.5, this phone number that was in the PayPal records, did you find that anywhere else in your investigation?

A Yes.

Q Now I'm going to show you what's been marked as Government's Exhibit 6.4.

Do you recognize this?

A Yes.

Q And this is a multi-page exhibit. How do you recognize Exhibit 6.4?

A This is a series of e-mails from a company called NuSphere, who was offering distributed denial service protection.

Q And did you find these in the rubensamvelich account?
A Yes, I did.
MR. BARBOSA: Government offers Exhibit 6.4.
MS. SCANLAN: One second.
THE COURT: Yes.
MS. SCANLAN: Counsel, all the pages?
MR. BARBOSA: All pages.
MS. SCANLAN: Your Honor, this exhibit contains communications between whoever the account holder is, of rubensamvelich, and this company. It appears other people -- I think this is hearsay. I would object to the admission of this exhibit.
THE COURT: Just one second, Counsel.
Counsel for the government?
MR. BARBOSA: Your Honor, primarily this consists of statements of a party opponent, for example, "This is my phone number," and other comments such as that. The responsive e-mails from the other party are only for context, not offered for the truth of the matter asserted. The username and password, there's no truth in them. They're just simply items that are located in the crime scene.
THE COURT: All right. Counsel for the defense, can you point to any particular aspects of the entirety of 6.4 that serve as a basis for your objection?
MS. SCANLAN: Your Honor, the first page of 6.4

consists entirely of an e-mail from someone else, who has not been identified, and we don't know the validity of this communication or if this is an accurate rendition of this information. I think to say that this isn't offered for the truth is a little confusing, considering what's actually sent from a company is a username and a password, not from the account holder, rubensamvelich.

MR. BARBOSA: To the extent that Page 1 is offered, that is also machine-generated information, as the witness has testified, so it's simply not hearsay. It's not a statement of a person. And a username and password carry no assertion or statement. They don't mean anything. They're simply a word that is found in the account.

THE COURT: Any other particular locations, Counsel, that you can point out to the Court?

MS. SCANLAN: Yes. One, I'm not sure how we know that Page 1 is machine generated. As to Page 2, there's a communication from an actual person at this company who has not been identified. We don't know who that is.

THE COURT: That's on Page 2?

MS. SCANLAN: Yes, Your Honor.

THE COURT: Bates Stamp 41?

MS. SCANLAN: Yes. Page 3 has the same kind of thing, another -- this is not a machine-generated e-mail. This is an e-mail to someone else. I don't know if Page 4 is

machine generated or not. I don't see any evidence that it is. Page 6 is not machine generated. They're e-mails from someone we don't know, to this account holder. I don't think these are business records, Your Honor.

THE COURT: All right. Counsel, I'll give the government an opportunity to establish foundation as it relates to Bates Stamp 22. That's 6.4, for ease of reference. Because I know the witness previously testified that they were machine generated in a global fashion, but not to the specifics of that particular exhibit page, Counsel. I would also note that on Page 2, again, same question, I'm not sure if sufficient foundation has been established to show that that's machine generated. You'll certainly be entitled to ask further questions. And the Court also has concerns and will sustain the objection as it relates to Page 6, because that appears not to indicate that that's machine generated, unless you can provide additional foundation.

MR. BARBOSA: Your Honor, Page 6 is a statement of the party opponent at the top. The bottom part is not offered for the truth. It actually doesn't have anything of important relevance. It's the statement of the defendant -- or statement of party opponent that is important on Page 6. I can lay a foundation for the machine generated.

THE COURT: Why don't you do that, Counsel. You can make another offering, and the Court will make a determination

at that point in time.
BY MR. BARBOSA
Q Are you familiar with how these types of receipts are created by a company such as NuSphere?
A Yes.
Q Does a person sit behind a keyboard and type out sign-in receipts like these?
A No.
Q How do you know that?
A Because I've never seen somebody do that in that fashion. It's much more -- it's easy to script this out to make it occur automatically. The formatting looks like it's automatically generated. The content and contact information at the bottom appears to me to be machine generated.
Q And are these the typical kind of messages you see in internet businesses when providing receipts?
A Yes. Additionally, it's not from a person's e-mail account. It's from a generic sales account.
MR. BARBOSA: Government offers 6.4 again.
THE COURT: Any other objections, Counsel?
MS. SCANLAN: Your Honor, I'm not sure I understand which page the witness is testifying about, at this point.
THE COURT: I took that as a global statement as to all six pages that were provided.
MS. SCANLAN: Yes, Your Honor. I would renew our

objection. I don't think -- one, generalized knowledge that he has seen e-mails of this nature from different businesses does not mean that he knows that these e-mails themselves are machine generated from this company. And in addition, some of these are very obviously not machine-generated e-mails.

THE COURT: Do you want to point out one, specifically, Counsel?

MS. SCANLAN: Page 2.

MR. BARBOSA: Your Honor, I can address this. We are not offering this for the truth of the matter asserted. It is a request for something to which the party replied. So what we are offering this for is the party opponent's statement.

THE COURT: All right. The Court will make the following determination.

Ladies and gentlemen of the jury, I'm going to admit 6.4 as offered by the government. You will note that there are communications that come from other individuals. And you'll see, for example, on Page 2, there's a reference to a Sergey, S-E-R-G-E-Y, Gitman. And you'll see the same applies on Page 3, and the same applies on Page 6.

The components of that statement that make reference to that person are not offered for the truth. It's only for purposes of explaining the basis of the communication. The Court will allow the balance of the testimony to come in, and you may consider it in its entirety otherwise.

So the objection is overruled. 6.4 is admitted.

(Exhibit 6.4 was admitted)

MR. BARBOSA: Thank you, Your Honor.

BY MR. BARBOSA

Q Who are the parties to this e-mail series?

A The e-mail account rubensamvelich@yahoo.com and the NuSphere.com company.

Q What is NuSphere?

A It's a company that provides distributed denial of service protection.

Q And is that the attack that you described earlier in your testimony?

A Yes.

Q So turning to Page 2 of Exhibit 6.4, what did the rubensamvelich account holder tell NuSphere about his phone number?

A He provides a phone number of +7902 -- I'll start again -- +79024835285. And it states, "This is my phone number."

Q Is that the same phone number you found in the PayPal record?

A Yes.

Q Turning back to Page 1 of Exhibit 6.4, do the username and password listed in this e-mail come up elsewhere in your investigation?

A Yes.

Q What were those?
A The username of track221 or track2, or a variation of that, was very common. And the password ochko123 was also very commonly used throughout the investigation.
Q Turning to Page 6 of Exhibit 6.4, what did the user of the rubensamvelich account say to the NuSphere Corporation?
A "What that mean, I am in Russia now. I live in Moscow. My billing address also Moscow, and now I am in other part of Russia. Any problems? If yes, just return my money to the card. I'm very disappointed of your service. Bye."
Q Did you contact NuSphere to obtain business records from them?
A Yes.
Q Showing you what's been marked as Government's Exhibit 15.14, which is two pages long, do you recognize that?
A Yes.
MR. BROWNE: 15.14?
MR. BARBOSA: Yes.
MR. BROWNE: Thank you.
MR. BARBOSA: The government offers those, again under a 902 certification.
THE COURT: Counsel?
MS. SCANLAN: Your Honor, if I may have just one moment?
THE COURT: You may.

Members of the jury, if you'd like to stretch, feel free to do so at this time.

Please be seated.

MS. SCANLAN: Your Honor, the defense has no objection.

THE COURT: 15.14 is admitted.

(Exhibit 15.14 was admitted)

BY MR. BARBOSA

Q Turning your attention to the NuSphere records, Page 1, Exhibit 15.14, do they have the same phone number on record?

A Yes, it does.

Q Was there anything else in the billing records they had for the rubensamvelich NuSphere account that you had seen elsewhere in your investigation?

A The "Roman Ivanov" name was there.

Q What about this address?

A It was also seen.

Q Where had you seen that before?

A Off the top of my head, I can't remember.

Q Okay. Let me draw your attention to Exhibit 4.12.

A That's right. It was for the account registration for -- I believe it was track2vip.tv and track2.tv.

Q So the same street address, but not number and apartment?

A Right.

Q Now I'm going to show you what's been marked as

Government's Exhibit 6.5.

Did you find other e-mails related to DDoS protection services?

A Yes.

Q Do you recognize Exhibit 6.5? This is a much longer exhibit. It's 22 pages, so you may want to look at it in the binder.

A This is which one?

Q 6.5.

A I need that binder. You said 6.15?

Q 6.5, sorry.

A I go from 6.22 to 7.1.

Q Oh, sorry. You may need another binder.

MR. BROWNE: You can use ours, if you want.

MR. BARBOSA: We'll use the originals.

May I approach, Your Honor?

THE COURT: Yes.

THE WITNESS: Okay. My math's not on point today. I apologize, Your Honor. Okay.

BY MR. BARBOSA

Q Do you recognize that?

A Yes.

Q How do you recognize it?

A These were records -- these are records that were found in the rubensamvelich@yahoo e-mail account from Prolexic.

Q Was this an e-mail that had contained an attachment also?
A Yes.
Q And is the e-mail and the attachment included in this exhibit?
A Yes.
MR. BARBOSA: Government offers Exhibit 6.5.
MS. SCANLAN: Your Honor -- I'm sorry. The defense objects as to 6.5 as to the communications that are not from the e-mail account holder.
THE COURT: They're not from the e-mail --
MS. SCANLAN: I apologize. So there's two people corresponding in this exhibit.
THE COURT: Right.
MS. SCANLAN: One of whom is the account holder.
THE COURT: Correct.
MS. SCANLAN: Who the government has offered as a party opponent.
THE COURT: Correct.
MS. SCANLAN: The other is not. And we believe the communications from that party are hearsay.
THE COURT: And counsel for the government?
MR. BARBOSA: Same response as Exhibit 6.4. They're only offered for context. They explain the responses from the party opponent.
THE COURT: Members of the jury, they'll be offered

for that limited purpose and that purpose only, and for no other reason.

6.5 will be admitted.

(Exhibit 6.5 was admitted)

BY MR. BARBOSA

Q So turning to Page 2 of 6.5, did the user provide a phone number and information about what he was looking for?

A Yes.

Q What?

A So the user provided a phone number of +79024835285, e-mail address of rubensamvelich@yahoo.com, and specifically in the message stated, "Hello, my site www.track2.tv is under very big DDoS attack. Now my DDoS protection from blacklotus.net, but they can't do anything to protect me already 24 hours. I very interested in your services. I need 100 percent guarantee if you can protect me from DDoS, because I also lose so much money. Thanks you. I would prefer to be contacted by e-mail."

Q So does Prolexic offer similar services to what NuSphere offers?

A Yes.

Q What name did the rubensamvelich account holder use when dealing with Prolexic?

A Roman Ivanov.

Q Now showing you what's been marked as Government's Exhibit 6.13, which is three pages, do you recognize these

three e-mails?
A Yes.
Q How do you recognize these three e-mails?
A These are e-mails between Black Lotus Communications, another DDoS provider, and rubensamvelich@yahoo.com.
Q Did any of these e-mails appear to be automatically receipts?
A Yes.
Q Which ones?
A The very first one.
Q What tells you that that was automatically generated?
A Based on the fact that it's from a support e-mail address, not from a user account, and the fact that it only contains the e-mail address and registration password, and no further details.
Q All right. The other two e-mails are two pages.
What do they include? What type of information, without going into the specifics?
A That they were specifically addressed to -- one was from Mr. Seleznev to them, with specific comments. And the second one was from them to him, with answers.
MR. BARBOSA: The government offers Exhibit 6.13 with the same conditions as 6.4 and 6.5.
MS. SCANLAN: Your Honor, the only objection I have is to 6.13, Page 3, which is the e-mail from Black Lotus

Communications support to the rubensamvelich e-mail account.

THE COURT: The Court will sustain the objection on Page 3 from the section that will be "Roman" down. That will not be admissible. Otherwise, 6.13 is admitted.

(Exhibit 6.13 was admitted)

MR. BARBOSA: Just a moment, Your Honor.

THE COURT: It appears the proper redaction has been made. You can make the offer once again, Counsel.

MR. BARBOSA: Thank you, Your Honor. And we will need to redact the original exhibit in the binders before they go to the jury.

THE COURT: That's fine.

BY MR. BARBOSA

Q All right. Let's turn to Page 1, first.

Do you see any passwords that you've seen elsewhere in your investigation?

A Yes. The ochko123.

Q Turning to Page 2, who is this message from?

A This is from rubensamvelich@yahoo.com.

Q And can you go over the message?

A Sure. It's to Black Lotus. And the content is "web proxy setup," is the subject. "I already paid by WebMoney, domain name www.track2.tv and track2.tv. No SSL or other certificates, only 80 port. Proxy must redirect to IP91.205.40.10. I waiting ASAP, because my site on DDoS

attack. Thanks you."

Q You had gone over the IP address for track2 earlier as an IP starting with "213."

What does this, "Proxy must redirect to IP," tell you?

A The true source IP address for the sites was 91.205.40.10.

Q Turning to Page 3 of Exhibit 6.13, who was this e-mail from and to?

A From rubensamvelich@yahoo.com.

Q And what was the subject of this?

A "Reference ticket ID 144705. Backend of track2.tv not responding."

Q And what did rubensamvelich tell Black Lotus?

A "Please disable permanent ban after multiple blocks. I have high-skilled administrator. He on ICQ. I can give you his ICQ to speak."

Q What would "administrator" be, in your training and experience, in this circumstance?

A So the first part of the e-mail addresses the fact that the way this was configured, they would permanently block IP addresses that they saw multiple times. So he wanted them to stop doing that, because he did want his administrator to be able to get in, and his administrator had been blocked. And then the second one is that he has somebody who is helping him with the sites, and that he is available to chat with them.

Q Did you contact Black Lotus to see if you could get

records from them?
A Yes.
Q Showing you what's been marked as Exhibit 15.4, do you recognize that?
A Yes.
Q How do you recognize this exhibit, which is four pages long?
A These are records that have been provided by Black Lotus.
MR. BARBOSA: The government's offering 15.4 under a 902 certification.
THE COURT: Counsel, you had a conversation with defense counsel. I didn't hear it. I'm not sure if the court reporter heard it.
MR. BARBOSA: Sorry. Government is offering 15.4 under a Rule 902 certification.
THE COURT: Let me hear from the defense.
MS. SCANLAN: Your Honor, if I may just take a look at it, briefly?
THE COURT: You may.
If you'd like to stand and stretch?
Please be seated.
MS. SCANLAN: The defense has no objection to this exhibit.
THE COURT: 15.4 is admitted.
(Exhibit 15.4 was admitted)

BY MR. BARBOSA

Q Okay. Turning to Page 2 of Exhibit 15.4, what do these records reflect in terms of the services that Black Lotus was providing for the rubensamvelich account?

A That they had Black Lotus, their elite proxy, for the domain track2.tv, and that it had a dedicated Black Lotus IP address.

Q Between these three sets of records related to DDoS protection, why were these important to you in your search through the rubensamvelich account?

A It showed that his infrastructure was under constant attack. It provided information related to where the servers that hosted the sites were also physically located. It also provided information on his true identity, through the phone number that was associated, as well as other methods of payment.

Q Turning to Page 3 of the exhibit, you mentioned methods of payment.

What method of payments did you see here?

A Liberty Reserve.

Q And what was the importance of Liberty Reserve or the WebMoney reference to your investigation?

A It just gave us another investigative track that we could follow from the perspective of those specific accounts. It also showed that he was using payment methods that are commonly

associated with the underground economy.
Q Turning to Page 4 of Exhibit 15.4, what name did the rubensamvelich account user use when dealing with Black Lotus?
A Roman Ivanov.
Q And the phone number, was that anywhere near the phone number you had seen before?
A Yes.
Q What -- how far off was it?
A It was off by just one digit. I think the last is a "2," instead of a "5."
Q So when dealing with all three of these DDoS protection services related to the track2 domains, we see that rubensamvelich was using the name Roman Ivanov.
MS. SCANLAN: Objection. Leading.
THE COURT: It is leading, Counsel.
BY MR. BARBOSA
Q Did you attempt to follow up on the name Roman Ivanov?
A Yes.
Q Any other names that you attempted to follow up on?
A Roman Seleznev.
Q How did you go about trying to follow up on those names?
A We looked for Western Union records related to those names.
Q Why did you ask Western Union to provide you with records?
A Number one, from bulbacc we knew that Western Union was a

method of payment that he was willing to accept. It's very commonly known -- commonly used payment mechanism to transfer monies around the globe. Secret Service had a relationship with Western Union for obtaining those records.

Q What did you ask Western Union to provide you with?

A All records and transfers related to those two names, Roman Ivanov and Roman Seleznev.

Q Did you include any other names that had come up in your investigation?

A Liudmila Bochkareva. I can't pronounce it.

Q Okay. We'll try and get some spelling for the court reporter later.

I'm showing you what's been marked as Government's Exhibit 15.2.

Do you recognize this exhibit? It's six pages long.

A Yes.

Q How do you recognize that?

A These are records that were provided by Western Union.

MR. BARBOSA: Government offers Exhibit 15.2 under a 902 certification.

MS. SCANLAN: No objection.

THE COURT: 15.2 is admitted.

(Exhibit 15.2 was admitted)

BY MR. BARBOSA

Q So we now have this on the screen in front of us. There's

quite a few names.

What format did Western Union provide this record in?

A It was an Excel spreadsheet.

Q And what kind of information did they provide?

A The date that the wire transfers were sent, the payee name, the city, the amount, the payee's date of birth, the payee's identification number, the ID place of issue, the date of issue, expiration, telephone number.

Q Did -- how many pages of data was this?

A Six.

Q What were you looking for in these six pages of Western Union records that you obtained?

A Anything that linked back -- linked those names to anything else in the rest of our case.

Q Okay. Were you looking for specific connections to the rubensamvelich account?

A Rubensamvelich account, the phone numbers that we'd seen, the names that we'd seen, geographical locations that we had seen.

Q Did you find any links between entries for Roman Ivanov names and the other items that you had looked at?

A No.

Q Did you find any links between any of the names and the rubensamvelich account?

A Yes.

Q What kind of links?
A We found links between the name "Roman Seleznev" and the phone number that we had seen.
Q Turning your attention to Exhibit 15.2A, do you recognize this?
A Yes.
Q How do you recognize that?
A This is a summary of the four transfers with the payee name "Roman Seleznev" that were related to the case.
Q So is this a summary, or is this just the data taken out of that larger spread --
A It's just the data taken out of the larger spreadsheet.
MR. BARBOSA: Government offers Exhibit 15.2A.
THE COURT: Any objection?
MS. SCANLAN: Is it offered for demonstrative purposes?
MR. BARBOSA: No. This is a substantive exhibit.
MS. SCANLAN: I would object to this as a substantive exhibit.
THE COURT: Counsel, let me ask the government, if 15.2A is extracted from 15.2, isn't that cumulative?
MR. BARBOSA: Well, we can look at 15.2, but we'll have to go through one line at a time, through six pages of data.
THE COURT: For the four entries?

MR. BARBOSA: Yeah.

THE COURT: All right. Are you offering it as cumulative [sic]?

MR. BARBOSA: I believe it's substantive evidence, because it is the exact same data, so it's not actually a summary. It's just only the entries for that particular name. It could, I guess, technically be considered a summary in the terms of it does offer the data in a more easy-to-review format.

THE COURT: All right. Counsel, if you want to offer it as an illustrative or demonstrative exhibit, I'll permit it under those grounds. Otherwise, it's overruled. But I will permit you to use 15.2A as a demonstrative exhibit, so it will not be going back to the jury room.

BY MR. BARBOSA

Q So are these lines, these four lines that we see in 15.2A, are they in the larger exhibit, 15.2?

A Yes.

Q You just need to thumb through each of the pages to find these?

A That's correct.

Q Okay. So what was the commonality you found between these four "Roman Seleznev" entries and other records you'd seen in your investigation?

A Primarily the name, as well as the telephone number

associated with the account. And then the pay agent city linked back to some IP addresses that we had seen, as well.

Q Did all four of these entries contain a similar ID number?

A Yes.

Q Okay. What -- in total, what data is excerpted in 15.2A, the demonstrative?

A So we have the date that the transfers were sent, the payee's name, the pay agent city, the recording amount in currency, the payee's date of birth for one of the entries, the ID type, the ID number, the place of issue, the issue date, and the expiration date for the ID, and then one also has a phone number.

Q I'll see if I can focus in on this. Bear with me for a minute.

Bringing up what's been previously admitted as Exhibit 12.7A, Page 21. And let me know if you can't see that. I can bring these up individually, but I have 15.2A on the left.

Is that the same ID number as found in the passport seized from Mr. Seleznev at the time of his arrest?

A Yes, it is.

Q And does it also have an expiration date, or an issue date, in some instances, for the passport?

A In one instance, it does have that, yes, for the issue date. It has expiration for all of them.

Q And did those match the passports seized from the defendant?
A Yes.
Q Again, the phone number, what did that match you'd seen elsewhere?
A It matched the records from the rubensamvelich e-mail account, specifically, that had been provided to some of the DDoS providers, as well as the PayPal records.
Q Moving back to the e-mails you found in the rubensamvelich account, did you find any other instances of the "smaus" or "ochko" username or password combinations in that account?
A Yes.
Q You have, in the binder in front of you, Exhibits 6.7, 6.8, and 6.8A. Can you tell me if you recognize those?
A You said 6.7 through 6.8?
Q 6.7 through 6.8A.
A Yes. Yes, I recognize these.
Q Let's start with 6.7. I'll go through this individually.
6.7 is approximately 20 pages long. What is the nature -- without going into the specifics, what is the nature of the e-mails that are included in Exhibit 6.7?
A The registration information and communications between rubensamvelich@yahoo.com and approvedinvest.com.
Q And there's 20 pages to that. I'd like you to go through these.

Are there similar -- again, without going into the specifics of what they are, I'd like to know the nature of these e-mails. What type of e-mails are they?

A The first one includes a login and password. The second one includes a statement about the username for the account holder. The third one, again, includes the account holder username. The fourth one is an automatic e-mail to -- regarding a recent transaction attempt and includes a username.

Q Are several of these automatic e-mails?

A Yeah. The majority of the ones towards the back are all automatic, state, "This is an automatic e-mail to inform you."

Q Based on the nature of the e-mails and the content, do they appear to be machine generated?

A All except for the bottom half of this Page 2.

MS. SCANLAN: Your Honor, if I may just show government counsel my copy, I just want to make sure we're looking at the same thing.

THE COURT: Certainly.

Members of the jury, if you'd like to stretch, please feel free to do so.

Ready, Counsel?

MS. SCANLAN: Yes, Your Honor.

THE COURT: All right. Are we on the same page of the same exhibit, Counsel?

MS. SCANLAN: We are on the same page of the same

exhibit, Your Honor. I'm objecting to 6.7. These -- the e-mail --

THE COURT: Just to be clear, 6.7, which particular pages? Because the witness has testified that some portions are automatically or machine generated. So I want to be very specific and precise.

MS. SCANLAN: Yes, Your Honor. We are not objecting to the first page, which is just labeled "6.7," otherwise known as "Yahoo! 1373."

THE COURT: Okay.

MS. SCANLAN: We are objecting to the second portion of Page 2 of 6.7, which is the second e-mail. There's a "from" e-mail, and then there's one below it. We're objecting to the one below it.

THE COURT: Can you tell me where it begins, Counsel? You don't have to read the whole thing.

MS. SCANLAN: Yes, Your Honor. From "invest at approvedinvest.com."

THE COURT: Okay. I'm with you.

MS. SCANLAN: To Page 4, the entirety of Page 4, hearsay objection. And I would note, it's not the same company as what's on Page 1 of 6.7. Same objection for 6.7, Page 6. This is also a different company than was on the first page. Page 8, same objection.

Page 10, Page 12, Page 14, Page 15 is a third "from," so

this is -- there are now three different senders of e-mails. I would also object to the relevance of Page 15 for the top of it, subject matter.

Page 16 is another e-mail from an unidentified business that's not the same as the prior pages. Same objection to Page 17. Page 18 is the same objection, Page 19 and Page 20.

THE COURT: Counsel for the government?

MR. BARBOSA: Your Honor, we're offering these only for the username and password indicated in here, which is a statement of party opponent. As the witness has already explained, these are user generated, and then the receipt is bounced back to them from the company with which he's -- the user is dealing with.

To the extent exhibits in 6.7 have party opponent statements, they come in under that, as not hearsay. The remainder of these e-mails are not at all -- the content of them is completely irrelevant and not offered for the truth of the matter asserted. The only thing of import is the username that repeatedly shows up in the account.

MS. SCANLAN: Your Honor, I would object, also, that a number of these, Page 20, Page 17 --

THE COURT: Counsel, why don't we excuse the jury so that we can get this exhibit clarified, and not have a running speaking objection between the two parties.

Members of the jury, I'm going to have you go back to the

jury room so we can get this resolved.

(Jury exits the courtroom)

THE COURT: Any objection to the witness remaining?

MS. SCANLAN: No, Your Honor.

THE COURT: All right, Counsel. Part of the concern I have, counsel for the government, is that there are several of these, as counsel has pointed out, without going back and saying individually, that they're all from different companies. And I don't know that the witness has gone as far to say that all the ones that were objected to were all machine generated, because some of these appear to come from -- well, they do appear to be from different companies. And I don't know that he's testified with sufficient foundation to establish that he's familiar with these particular companies to be able to identify that that would lead him to the conclusion, based upon training and experience, that these are machine generated.

MR. BARBOSA: We could go through each one. This should have probably been subject to a motion in limine before the deadline. Counsel has had these since February of this year.

But the government can offer testimony on each exhibit, individually. I believe this witness is qualified to testify based on the content and appearance of these exhibits. This is something that comes in under Rule 104, and the government's burden here is only to show authenticity, which is less than a

preponderance. We have to show what it purports to be. And that can be done without reference to the rules of evidence.

We can definitely go through these. Many of them actually indicate that they are automatically generated. I'm trying to find one, in particular, right now.

THE COURT: Well, for example, "08" says, "This is an automatic e-mail."

MR. BARBOSA: Exactly. Almost all of them have this, for example, Page 4, "This is an automatic e-mail."

THE COURT: All right. Counsel for the defense?

MS. SCANLAN: Your Honor, I would ask, unfortunately, that if they're lumped together like this, that these -- this is not one exhibit. These are all separate individual things.

And so, for instance, like, Page 17, the defense has an objection to the content of this e-mail being admitted. Whether it's for the truth or not, it's prejudicial to Mr. Seleznev.

THE COURT: How is it prejudicial, Counsel?

MS. SCANLAN: It's an e-mail from LivePimpin to rubensamvelich, who they are saying is the party opponent. And if you look at the e-mail address of the verification process that's copied in and the information that e-mail address -- I don't see the relevance of that to -- if this is really all about usernames and passwords, then the rest of this information isn't necessary to the government's case.

THE COURT: Counsel?

MR. BARBOSA: I don't really have a problem with redacting some of this information out. I think that the prejudice to the defendant, in a case where he's charged with stealing $170 million, is pretty minimal. But if that is -- if the Court thinks that would be appropriate, I don't believe we have any objection to excluding the e-mail address for the sender.

THE COURT: Okay. I think that's appropriate, Counsel. Because again, part of what the government's characterizing, as well, is lifestyle. And there are certain exhibits that come before the Court that show the defendant in various positions, various countries, volumes of money, currency in his possession. And I think the characterization of a website such as LivePimpin and then the website that says www.fucktheprincess.com is certainly potentially prejudicial to the defendant. It's not a question of the degree of prejudice. It's a question of prejudicial information. I find that that would be substantially more prejudicial than probative. So the Court will sustain the objection in that regard.

So the document can come in, but you need to make certain redactions, Counsel.

MS. SCANLAN: And Your Honor, the defense has the same objection to Page 15 regarding the content.

THE COURT: Just a second. Let me catch up with you.

All right. Counsel, the specific objection to what portion?

MS. SCANLAN: Page 15 is from the "adult community." And then it's talking about performances, quote, "If you want to see something a little more hardcore, you can enter XXX chat with the performers. The XXX chat is billed at a premium rate that is determined by each performer."

THE COURT: All right. Counsel for the government, any other basis to have that admissible?

MR. BARBOSA: No.

THE COURT: All right. Then the Court will direct that you redact that portion, as well. And again, we're talking about a specific line that says "adult community," and we're talking about the specific line that begins, "If you want to see something a little bit more hardcore"; so it's just those two lines, as well as the "adult community" reference.

Counsel for the defense, any other specifics?

Also, Counsel, let's strike "adult community," which is the last line on that same page.

MS. SCANLAN: Page 16, is from CamBooth.com. It has the same line, "If you want to see something a little more hardcore, you can enter XXX chat with the performers. The XXX chat is billed at a premium rate that is determined by each performer."

THE COURT: Counsel, I can accept your argument as it

relates to "something a little more hardcore." But "CamBooth" is such an innocuous term, I don't find that that's anywhere close to something like "LivePimpin," or the other references that were noted.

So I'll direct the government to redact the same line that begins, "If you want to see something a little more hardcore." But other than that, I don't see anything else that warrants the degree of prejudice that you've claimed.

Any other specific pages, Counsel?

MS. SCANLAN: Your Honor, Page 20.

THE COURT: Did we cover 17?

MS. SCANLAN: Yes. That's the "LivePimpin" page.

THE COURT: Okay. All right. Then that one's -- the Court's directed the redactions on that one.

And then 20?

MS. SCANLAN: "If you're craving a more intimate encounter, that's our specialty. Our video stars are" --

THE COURT: What paragraph, Counsel?

MS. SCANLAN: I'm sorry, Your Honor. It's paragraph -- well, after the usernames, it's one, two, three, four, five.

THE COURT: Okay.

MS. SCANLAN: So, "If you're craving a more intimate encounter, that's our specialty. Our video stars are here to please and perhaps tease you. Check out who's live right now."

I do think that the average reader is going to understand what that is about in the context of this e-mail.

And the same objection as to the pictures at the bottom of the e-mail, which include -- I believe that's a woman's breast, through a keyhole.

THE COURT: Okay.

MS. SCANLAN: And with the exception of the automated e-mails, the ones that say that they're automated, I renew our hearsay objection regarding the rest of them.

THE COURT: On 20, the Court will direct the government to make the redaction, "Do you desire some more intense imagery?" those two lines. The next one, "If you're craving a more intimate encounter," the Court will direct the government to -- actually, Counsel, I'm not sure of the relevance of the bottom portion of that. Everything below, "Enjoy some of our exclusive features below," a live cam spy, and the photographs, as well as the keyhole imagery, that should be redacted, as well.

MR. BARBOSA: How about we just redact everything below, "Why wait? Login now"? That may be the safest.

THE COURT: Okay. That's easier. That's fine with the Court.

All right. I think the Court's ruled on all the defense objections.

And counsel for the defense, if you're aware of any other

objections like this -- because I agree with the government. These types of redactions, the offering -- you've had these exhibits for a period of time -- could have been done sometime before, so we don't have to have these delays during the course of trial to address these particular objections. I'm not saying they're not valid objections, but these are things that we shouldn't be wrestling with in front of the jury for protracted periods of time.

So if you have any more, with counsel letting you know which witnesses are going to testify, you can look at these exhibits over the evening hours to make sure that you can bring it to the Court's attention at the beginning of the day, so that we don't have to have interruptions during trial to address this.

So counsel for the government, if you want to go through these exhibits with the jury present, you'll have the opportunity to do so. For those that there are no objection which the Court sustained, you can show those images or have the witness testify to them. But for those that require redaction, since you don't have to do the redactions right now, just show those portions which the Court has permitted; okay?

MR. BARBOSA: I do want to make sure that -- we have about 20 minutes. I just want to make sure nothing else that we are about to try and admit will require additional issues.

6.8A, I don't believe that has anything problematic.

MS. SCANLAN: No. And Your Honor, if the government could identify the exhibits it intends to admit the following day, then I will go through them in advance.

THE COURT: Well, I'll leave that to the parties, after we break for the day, to do that. But I think, Counsel, that would help speed it up for the government, as well.

MR. BARBOSA: The next ones are the iTunes receipts, 6.6.

MR. BROWNE: What was that one? I'm sorry.

MR. BARBOSA: 6.6. 6.17 is the next exhibit after that. And --

THE COURT: Counsel, we're not recording this. So if you two want to have a conversation about what you're going to be offering, that's fine. But the court reporter is instructed not to record those communications.

(Off the record)

THE COURT: Counsel, have you gone through the balance of the exhibits that you plan on offering for, say, the next 15 minutes?

MR. BARBOSA: I think I've gotten through the rest of the day here.

THE COURT: Counsel for the defense, do you have any particular objections that we can deal with now?

MS. SCANLAN: Did you just take that piece out of the iTunes charges?

MR. BARBOSA: Yes.

MS. SCANLAN: No, I don't have any objection.

THE COURT: Okay. Let's bring in the jury.

(Jury enters the courtroom)

THE COURT: Thank you, members of the jury. We've gone through the exhibits that will be offered for the balance of the day, so we shouldn't have any additional interruptions. Thank you.

MR. BARBOSA: Thank you.

BY MR. BARBOSA

Q Detective Dunn, we were talking about Exhibit 6.7.

MR. BARBOSA: The government now offers 6.7 with the conditions as we just went over.

THE COURT: All right. Any objections now, Counsel?

MS. SCANLAN: Your Honor, I understand the Court's ruling, but we still object on the hearsay basis.

THE COURT: Overruled on those grounds. Otherwise, 6.7 is admitted, subject to the Court's rulings.

(Exhibit 6.7 was admitted)

BY MR. BARBOSA

Q Detective Dunn, can you explain -- this is 20 pages of e-mails. What did you -- why did you select these 20 e-mails to highlight as exhibits?

A These were e-mails that were sent to the rubensamvelich@yahoo.com, from various providers of internet

websites, and they all contained a similar login name and password.

Q Why did that get your attention?

A People tend to become creatures of habit when it comes to usernames and passwords. So it, again, linked those usernames and passwords to the user.

Q So starting with Page 1, what was this username and password that you began to focus on?

A The login was "smaus1" and password of "ochko123."

Q Page 2, do you see that again?

A Yes.

Q Can you just read these in as we go through?

A "My username is smaus1."

Q Page 3?

A Username smaus1.

Q And that's from the user of the account to --

A That's from the user of the account to approvedinvest.com.

Q Page 3?

A This is an automatic e-mail from help@lalibcosupport.com, with a username of smaus123.

Q Page 6?

A This is another e-mail from lalibcosupport to username smaus123.

Q Page 7?

A Again, one from lalibcosupport to username of smaus321.

Q Page 10?
A Another one from that same e-mail address to a username smaus321.
Q Twelve?
A Another one from lalibcosupport.com to username smaus321.
Q Looks like you had at least one more from lalibcosupport.
Moving on to Page 15, what is this?
A This is from another provider, wcbilling.com. The username is smaus1234, the password of ochko123.
Q Page 16?
A Another one from webcams.com to username smaus123, password of ochko123.
Q Page 17?
A From another e-mail account to rubensamvelich, with the username of smaus123 and a password of ochko123.
Q Eighteen?
A Another one from support@InsidePro.com with a username of ruben123 and a password of ochko123.
Q Nineteen?
A One from info@ -- I can't read the whole e-mail address -- but a username of zagreb123235 with a password of ochko123.
Q And finally, the last one?
A Is an e-mail from iFriendsV2 support with an assigned username of alabus1 with a password of ochko123.
Q Did you look for these username and password combinations,

including the few that we saw that were slight variations, "ruben" and "zagreb," at other points in your investigation?

A Yes.

Q Did you find them anywhere else as you conducted your investigation?

A Yes.

Q Where?

A The username "smaus" was used extensively throughout the infrastructure. So the server hosting the malware had a domain name of smaus.fvds.ru. The "smaus" name showed up repeatedly throughout the investigation, as well as the "ochko123" password.

Q Did you also find receipts for iTunes purchases in the rubensamvelich account?

A Yes.

Q Showing you what's been marked as Government's Exhibit 6.6, which is three pages long, do you recognize that?

A Yes.

Q How do you recognize those?

A These are iTunes receipts that were in the rubensamvelich@yahoo.com account.

Q And are these automated receipts, based on the content?

A Yes.

Q How do you know?

A All iTunes receipts are automated.

MR. BARBOSA: Government offers 6.6.

MS. SCANLAN: No objection.

THE COURT: 6.6 is admitted.

(Exhibit 6.6 was admitted)

BY MR. BARBOSA

Q Why did you focus on these iTunes receipts?

A For a number of reasons. Apple would have records related to the device -- potentially have records related to the device that the user had. They were U.S.-based accounts that were used to make these purchases, as well as the specific apps could provide some context as to the user and their behavior.

Q I've highlighted the first page.

What were the purchases that you focused on here?

A The purchase I most focused on was "Tupac Greatest Hits."

Q Was that a focus during the original investigation, in 2010?

A No.

Q When did that come up?

A That came up after Mr. Seleznev's arrest.

Q Turning to the second page, anything in here that you focused on?

A The Item Number 2 and 3, the Luxe Bali City Guides mobile edition and the Bali Traveler applications.

Q Why did these draw your attention?

A We had a number of indications of travel to Bali, as well

as IP addresses that returned to the Denpasar, Bali, Indonesia area.

Q Was that also something showing up in the Western Union records?

A Yes.

Q When you say IP addresses that return to the Denpasar, Indonesia, area, what do you mean?

A So we found IP addresses both from the rubensamvelich e-mail account, as well as IP addresses located within the HopOne server that resolved back to Indonesia.

Q And when you say "located within the HopOne server," what do you mean? By logging in or --

A There were logins, yes.

Q And is that the server in the lower right-hand corner of the Exhibit 17.7?

A That's correct.

Q These are addressed to Anna Chamot. Who is that?

A She's an elderly woman who lives in the Washington, D.C. area.

Q And finally, Page 3 of this exhibit, the iTunes receipts in the rubensamvelich account, anything in here that you focused on?

A The voice changer applications, Fake-a-Call, and the translation applications.

Q I'm going to show you Exhibit 6.17. Do you recognize

this, which is one page?
A Yes.
Q Did you find that, also, in the rubensamvelich account?
A Yes.
Q And was this an automated e-mail, also?
A Yes.
MR. BARBOSA: Government offers Exhibit 6.17.
MS. SCANLAN: No objection.
THE COURT: It's admitted.
(Exhibit 6.17 was admitted)
BY MR. BARBOSA
Q What was the subject of this e-mail?
A "Review of your order required, multi-password recovery, share-it! Order Number 348102785."
Q Based on your training and experience, do you know what the multi-password recovery tool is?
A Yes. It's a tool for trying to recover passwords.
Q Switching gears a little bit, you described domain registration records.
Did you find anything in the e-mail accounts, related to the domain registration records, that had drawn your attention to the rubensamvelich account?
A Yes.
Q What did you find?
A The receipts for the registration of -- registration of a

number of different web domains associated with the nic "track2."

Q Can you look, in the binders in front of you, at Exhibits 6.9 through 6.10A?

A Okay.

Q Do you recognize those?

A Yes.

Q What's the nature of those exhibits in 6.9 through 6.10A?

A It's the account creation for WebNames.ru, which is a Russian-based domain name registrar, as well as for the registration of a number of domain names.

Q And were those all in the rubensamvelich account?

A Yes.

MR. BARBOSA: Government offers Exhibits 6.9 through 6.10A.

MS. SCANLAN: No objection.

THE COURT: They're all admitted.

(Exhibits 6.9 through 6.10A were admitted)

BY MR. BARBOSA

Q All right. Let's first look at Exhibit 6.9A, which is the translation of the original in 6.9.

When was this dated?

A September 10, 2009.

Q Did that match up with the domain registration records you reviewed earlier?

A Yes.
Q So what was this for?
A For the domain registration to track2.tv.
Q Is that what I've highlighted here?
A Yes.
Q So did this confirm that this account was being used to manage the domain?
A Yes.
Q Moving on to 6.10A, what do we have here?
A So this is for the registration to the actual WebNames.ru portal. So this is to gain access to their portal to then register names, so with a login of track2 and password of smaus123.
Q What is WebNames.ru?
A So WebNames.ru is a Russian-based domain name registrar, so a company that can register domain names.
Q And do you recognize the login or password here?
A Yes.
Q What are they?
A Track2 and smaus123.
Q Moving on to the second page of Exhibit 6.10A, what is this e-mail here?
A It's for the domain registration for track2.name.
Q Is that one of the alternate websites that you had referred to?

A Yes.
Q And if you move on to Exhibit 6.14, do you recognize this exhibit, which is just one page?
A Yes.
Q And there's the translation, 6.14A.
How do you recognize this?
A This is in an e-mail from HostTracker showing the daily statistics for the website track2.tv.
MR. BARBOSA: Government offers Exhibits 6.14 and 6.14A.
MS. SCANLAN: No objection.
THE COURT: They're both admitted.
(Exhibits 6.14 and 6.14A were admitted)
BY MR. BARBOSA
Q What is this e-mail about?
A This shows that the overall up-time, or availability, for the website track2.tv was 99.9 percent, meaning that throughout the previous 24-hour period, the site was pretty much up the entire time and available to customers.
Q And based on your training and experience, what is the purpose of a HostTracker report? Why would somebody want something like this?
A It's so that a website owner can ensure and validate that his site is available to clients. So if you saw something under 99.9 percent, then there may be an issue with your web

hoster, or a DDoS attack, or something else going on.

Q And had you seen indication that these sites were under DDoS attack?

A Yes.

MR. BARBOSA: Your Honor, I'm about to move into a new section. I don't know if the Court wants me to keep going right now? I'm happy to.

THE COURT: We'll break at this time.

Members of the jury, have a good evening. Again, same instructions that you received yesterday about not reading anything, same goals and objectives to keep your mind free of all taint of outside influences.

So have a great evening. The weather straightened out. It's about 80-plus degrees. We'll see you all tomorrow morning at 9:00 a.m. Have a good evening.

(Jury exits the courtroom)

THE COURT: Counsel for the government, anything to take up?

MR. BARBOSA: No, Your Honor. Thank you.

THE COURT: Counsel for the defense?

MS. SCANLAN: No, Your Honor.

THE COURT: Have a good evening. See you all tomorrow morning at 9:00.

(Adjourned)

(End of requested transcript)

* * *

I certify that the foregoing is a correct transcript from the record of proceedings in the above matter.

Date: 8/16/16 /s/ Andrea Ramirez

Signature of Court Reporter